

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-173381

(P2003-173381A)

(43) 公開日 平成15年6月20日 (2003. 6. 20)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト* (参考)
G 0 6 F 17/60	1 4 2	G 0 6 F 17/60	1 4 2 5 B 0 1 7
	3 0 2		3 0 2 E 5 B 0 8 5
12/14	3 2 0	12/14	3 2 0 F 5 J 1 0 4
15/00	3 3 0	15/00	3 3 0 B
			3 3 0 Z

審査請求 未請求 請求項の数22 O L (全 60 頁) 最終頁に続く

(21) 出願番号 特願2002-154341(P2002-154341)

(22) 出願日 平成14年5月28日 (2002. 5. 28)

(31) 優先権主張番号 特願2001-160290(P2001-160290)

(32) 優先日 平成13年5月29日 (2001. 5. 29)

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願2001-224413(P2001-224413)

(32) 優先日 平成13年7月25日 (2001. 7. 25)

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願2001-291593(P2001-291593)

(32) 優先日 平成13年9月25日 (2001. 9. 25)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 大穂 雅博

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 上坂 靖

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100098291

弁理士 小笠原 史朗

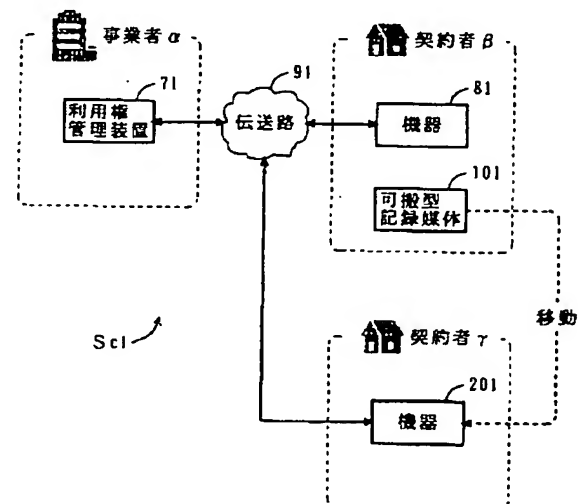
最終頁に続く

(54) 【発明の名称】 利用権管理装置

(57) 【要約】

【課題】 他者の機器上で、自分の利用権情報を使って、コンテンツデータを利用可能な利用権管理装置を提供すること

【解決手段】 契約者αの機器201は、契約者βの可搬型記録媒体101内のメディア識別子を使って、コンテンツデータの利用許可を受けるための発行要求を生成し、利用権管理装置71に送信する。利用権管理装置71は、契約者βに与えられたコンテンツデータの利用権情報を管理し、当該利用権情報と、発行要求とを使って、可搬型記録媒体101にコンテンツデータの利用を許可する利用許可情報を生成する。さらに、利用権管理装置71は、利用許可情報に基づいて、可搬型記録媒体101に接続された機器におけるコンテンツデータの利用を制御するライセンス情報を生成して、機器201に送信する。機器201は、ライセンス情報を処理して、コンテンツデータの利用を制御する。



【特許請求の範囲】

【請求項1】 複数の機器がコンテンツデータを利用するための権利を表す利用権情報を管理するための装置であって、
前記複数の機器に割り当てられる利用権情報を含む利用権データベース（以下、利用権DBと称する）と、
各前記機器からの発行要求にตอบสนองして、前記利用権DBに含まれる利用権情報を使って、発行要求を送信した機器に対するコンテンツデータの利用許可を示す利用許可情報を生成する利用権管理部と、
前記利用権管理部で生成された利用許可情報を少なくとも含むライセンス情報を生成するライセンス情報生成部と、
前記ライセンス情報生成部で生成されたライセンス情報を、発行要求を送信した機器に送信する通信部とを備える、利用権管理装置。

【請求項2】 前記機器は、コンテンツデータの利用条件を少なくとも含む設定要求を送信し、
前記利用権管理部は、前記機器からの設定要求にตอบสนองして、少なくとも設定要求を送信した機器に対する利用権情報を前記利用権DBに登録する、請求項1に記載の利用権管理装置。

【請求項3】 前記複数の機器は予め定められたグループに属しており、
前記利用権管理部は、前記グループに属する1台の前記機器からの設定要求にตอบสนองして、グループに属する各機器により共有される利用権情報を前記利用権DBに登録する、請求項2に記載の利用権管理装置。

【請求項4】 配信対象となるコンテンツデータを蓄積するコンテンツデータベース（以下、コンテンツDBと称する）をさらに備え、
前記機器が送信する設定要求はさらに、取得対象のコンテンツデータを特定しており、
前記機器からの設定要求にตอบสนองして、コンテンツDBから、取得対象のコンテンツデータを読み出すコンテンツ管理部と、
前記コンテンツ管理部で読み出されたコンテンツデータを暗号化するコンテンツ暗号化部と、
前記コンテンツ暗号化部で暗号化されたコンテンツデータを含む送信データを生成する送信データ生成部とをさらに備え、
前記通信部はさらに、前記送信データ生成部で生成されたデータを、設定要求を送信した機器に送信する、請求項2に記載の利用権管理装置。

【請求項5】 前記コンテンツ暗号化部で暗号化されるコンテンツデータを復号するための復号鍵を含む復号鍵データベース（以下、復号鍵DBと称する）をさらに備え、

前記ライセンス情報生成部は、前記復号鍵DB内の復号鍵をさらに含むライセンス情報を生成する、請求項1に

記載の利用権管理装置。

【請求項6】 前記復号鍵DB内の復号鍵を、発行要求を送信した機器に関連する情報で暗号化する復号鍵暗号化部をさらに備え、

前記ライセンス情報生成部は、前記復号鍵暗号化部で暗号化された復号鍵をさらに含むライセンス情報を生成する、請求項5に記載の利用権管理装置。

【請求項7】 前記ライセンス情報生成部は、前記利用権管理部で生成された利用許可情報に基づいて、ライセンス情報の改竄を防止するためのハッシュ値を生成するハッシュ値生成部と、
前記ハッシュ値生成部で生成されたハッシュ値を、前記利用権管理部で生成された利用許可情報に付加して、ライセンス情報を組み立てるライセンス情報組立部とを含む、請求項1に記載の利用権管理装置。

【請求項8】 前記利用権管理部は、発行要求の送信元となる機器のために利用許可情報を生成できない場合には、利用拒否情報を生成し、

前記通信部はさらに、前記利用権管理部で生成された利用拒否情報を、発行要求の送信元となる機器に送信する、請求項1に記載の利用権管理装置。

【請求項9】 予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報DBと称する）と、
前記ユーザ情報DBに未登録の機器識別子を有する機器からの登録要求にตอบสนองして、受信登録要求に含まれる未登録の機器識別子を前記ユーザ情報DBに登録するユーザ情報管理部とをさらに備える、請求項1に記載の利用権管理装置。

【請求項10】 前記ユーザ情報管理部は、1グループに登録されている機器識別子数が、予め定められた上限値以上である場合には、登録要求にตอบสนองして、前記ユーザ情報DBへの登録を拒否するための登録拒否通知を生成し、
前記通信部はさらに、前記ユーザ情報管理部で生成された登録拒否通知を、登録要求の送信元となる機器に送信する、請求項9に記載の利用権管理装置。

【請求項11】 予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報DBと称する）をさらに備え、

前記ユーザ情報DBに登録済の機器は、自身の機器識別子を登録対象識別子として少なくとも含む仮登録要求を送信し、
受信仮登録要求に含まれる登録対象識別子を前記ユーザ情報DBに仮登録するユーザ情報管理部をさらに備え、
前記ユーザ情報DBに未登録の機器は、登録対象識別子と、仮登録要求の送信元となった機器の機器識別子である登録済識別子とを少なくとも含む本登録要求を送信し、

10

20

30

40

50

前記ユーザ情報管理部は、受信本登録要求に含まれる登録対象識別子および登録済識別子に基づいて、前記ユーザ情報DBに仮登録された登録対象識別子を本登録する、請求項1に記載の利用権管理装置。

【請求項12】 予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報DBと称する）をさらに備え、

前記ユーザ情報DBに未登録の機器は、自身の機器識別子を登録対象識別子として含み、さらに、登録済の機器識別子を含むパスワード要求を送信し、

受信パスワード要求に含まれる登録対象識別子を前記ユーザ情報DBに仮登録し、さらに、未登録の機器に対するパスワードを発行するユーザ情報管理部をさらに備え、

前記ユーザ情報DBに未登録の機器は、登録対象識別子と、前記ユーザ情報管理部により発行されたパスワードとを含む登録要求を送信し、

前記ユーザ情報管理部は、受信登録要求に含まれるパスワードと登録対象識別子とに基づいて、前記ユーザ情報DBに仮登録された登録対象識別子を本登録する、請求項1に記載の利用権管理装置。

【請求項13】 予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報DBと称する）をさらに備え、

前記ユーザ情報DBに未登録の機器は、自身の機器識別子を登録対象識別子として少なくとも含む第1の登録要求を、ユーザ情報DBに登録済の機器に送信し、

前記ユーザ情報DBに登録済の機器は、自身の機器識別子を登録済識別子として含み、さらに、受信した第1の登録要求に含まれる登録対象識別子を含む第2の登録要求を送信し、

受信した第2の登録要求に含まれる登録対象識別子を前記ユーザ情報DBに登録するユーザ情報管理部をさらに備える、請求項1に記載の利用権管理装置。

【請求項14】 前記利用権DBには、利用権情報と、その利用権情報を利用可能な機器の機器識別子とが登録されており、

予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報DBと称する）と、

各前記機器からの削除要求にตอบสนองして、前記ユーザ情報DBおよび前記利用権DBから機器識別子を削除する機器識別子削除部とをさらに備える、請求項1に記載の利用権管理装置。

【請求項15】 前記複数の機器は予め定められたグループに属しており、

前記利用権管理部は、

前記グループに属する第1の機器からの設定要求にตอบสนอง

して、設定要求の送信元となる第1の機器の利用権情報を前記利用権DBに登録し、

前記グループに属する第2の機器からの設定要求にตอบสนองして、設定要求の送信元となる第2の機器を、第1の機器の利用権情報と共有可能に前記利用権DBに登録する、請求項2に記載の利用権管理装置。

【請求項16】 伝送路を通じて接続された利用権管理装置から、ライセンス情報の提供を受ける機器であって、

前記機器は、

自身を一意に特定するメディア識別子を格納する可搬型記録媒体をデータ通信可能に接続するインターフェイスと、

前記インターフェイスに接続された可搬型記録媒体からメディア識別子を取り出す識別子抽出部と、

前記識別子抽出部から受け取るメディア識別子を使って、コンテンツデータの利用許可を受けるために必要な発行要求を生成する発行要求生成部と、

前記発行要求生成部から受け取る発行要求を、前記伝送路を通じて、前記利用権管理装置に送信する第1の通信部とを備え、

前記利用権管理装置は、

前記可搬型記録媒体に与えられたコンテンツデータの利用権情報を管理しており、前記機器からの発行要求にตอบสนองして、前記可搬型記録媒体が接続された機器におけるコンテンツデータの利用を制御するためのライセンス情報を生成して送信し、

前記機器はさらに、

前記利用権管理装置からのライセンス情報を処理して、コンテンツデータの利用を制御するライセンス情報処理部とを備える、機器。

【請求項17】 前記利用権管理装置は、前記機器がコンテンツデータを利用するための最低限度の利用許可情報を生成する利用権管理部を備える、請求項16に記載の機器。

【請求項18】 前記利用権管理装置は、

ライセンス情報を生成するために、前記利用権管理部で生成された利用許可情報に基づいて、第1のハッシュ値を生成する第1のハッシュ値生成部と、

前記第1のハッシュ値生成部から受け取る第1のハッシュ値を、前記利用権管理部から受け取る利用許可情報に付加して、ライセンス情報を組み立てるライセンス情報組立部とを含む、請求項17に記載の機器。

【請求項19】 前記ライセンス情報処理部は、

受信ライセンス情報に含まれる利用許可情報に基づいて、第2のハッシュ値を生成する第2のハッシュ値生成部と、

前記第1の通信部から受け取るライセンス情報に含まれる第1のハッシュ値と、前記第2のハッシュ値生成部から受け取る第2のハッシュ値とに基づいて、

前記第1の通信部から受け取るライセンス情報に含まれる利用許可情報が改竄されているか否かを判定する改竄判定部とを含む、請求項18に記載の機器。

【請求項20】 前記コンテンツデータは、前記機器に、予め定められた暗号鍵で暗号化された状態で配信され、

前記ライセンス情報組立部はさらに、前記利用権管理部から受け取る発行要求からメディア識別子を取り出し、前記利用権管理装置は、

前記暗号鍵で暗号化されたコンテンツデータを復号可能な復号鍵を管理する復号鍵管理部と、

前記復号鍵管理部で管理される復号鍵を、前記ライセンス情報組立部により取り出されたメディア識別子で暗号化する復号鍵暗号化部とをさらに備え、

前記ライセンス情報組立部はさらに、前記復号鍵暗号化部から受け取る暗号化された復号鍵を、前記利用権管理部から受け取る利用許可情報に付加して、ライセンス情報を組み立てる、請求項18に記載の機器。

【請求項21】 前記ライセンス情報処理部は、前記識別子抽出部から受け取るメディア識別子を使って、前記第1の通信部から受け取るライセンス情報に含まれる暗号化された復号鍵を復号する復号鍵復号部をさらに備える、請求項20に記載の機器。

【請求項22】 自身に割り当てられた機器識別子を格納するための機器識別子格納部をさらに備え、

前記識別子抽出部は、ユーザの操作に応じて、前記インターフェイスに接続された可搬型記録媒体からメディア識別子を取り出すか、前記機器識別子格納部から機器識別子を取り出すかを決定する、請求項16に記載の機器。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、利用権管理装置に関し、より特定的には、コンテンツデータに関連する権利を管理する利用権管理装置に関する。

【0002】

【従来の技術】近年、ネットワークのブロードバンド化および常時接続環境により、コンテンツ配信システムが身近なものになりつつある。また、このようなコンテンツ配信システムの普及には、コンテンツデータに関連する権利の保護が重要であることから、従来から、様々な権利管理技術の研究および開発がなされている。ここで、本願明細書では、著作権または販売権のようなコンテンツデータに関連する権利を、デジタルライツと称する。以下、従来の権利管理技術を組み込んだコンテンツ情報配信システムについて説明する。

【0003】従来のコンテンツ配信システムには、コンテンツ配信装置と、パーソナルコンピュータ（以下、PCと略記する）とが、インターネットに代表されるネットワークにより、データ通信可能に接続される。コンテ

ンツ配信装置は、コンテンツデータ、コンテンツ復号鍵および利用条件データの組みを少なくとも1つ格納している。コンテンツデータは、例えば、音楽に代表されるコンテンツを表すデジタルデータであり、予め定められた方式で暗号化される。コンテンツ復号鍵は、暗号化されたコンテンツデータを復号するための鍵である。利用条件データは、上述のコンテンツデータの利用可能な条件（以下、利用条件と称する）を表すデータである。利用条件としては、コンテンツデータの利用回数が代表的である。PCは、上述のコンテンツデータをコンテンツ配信装置から取得し、さらに、取得したコンテンツデータを利用するために必要なコンピュータプログラム（以下、単にプログラムと称する）を格納している。

【0004】以上のコンテンツ配信システムでは、以下のようにして、コンテンツデータが配信される。まず、PCは、予め格納されているプログラムを実行して、コンテンツデータの配信をコンテンツ配信装置に要求する。コンテンツデータの要求は、一般的に、コンテンツ特定情報および端末固有情報を、PCがネットワークを介してコンテンツ配信装置に送信することで行われる。コンテンツ特定情報は、上述のコンテンツデータを一意に特定する情報である。端末固有情報は、PCにより予め保持されており、上述のコンテンツデータの要求元であるPCを一意に特定可能な情報である。

【0005】コンテンツ配信装置は、PCからの要求に応答して、上述のコンテンツ復号鍵を、今回受信した端末固有情報を使って暗号化する。その後、コンテンツ配信装置は、上述の暗号化されたコンテンツデータと、端末固有情報で暗号化されたコンテンツ復号鍵と、利用条件データとをPCに送信する。PCは、コンテンツ配信装置により配信されたコンテンツデータ、コンテンツ復号鍵および利用条件データを受信し、内部に備える記憶装置に格納する。

【0006】以上の格納後、PCのユーザは、コンテンツデータを復号することで、それが表すコンテンツを出力可能な状態になる。実際にコンテンツを出力するまでには、ユーザは最初に、その旨をPCに指示する。この指示に応答して、PCは、以下のように動作する。PCは、記憶装置内の利用条件データにより表される利用条件に、今回の利用が台致しているか否かを判定する。PCは、利用条件に台致する場合に限り、以下の処理を実行する。次に、記憶装置内のコンテンツ復号鍵は暗号化されているので、PCは、自身が保持する端末固有情報を使って、当該コンテンツ復号鍵を復号する。さらに、記憶装置内のコンテンツデータもまた上述のように暗号化されているので、PCは、復号したコンテンツ復号鍵を使って、当該コンテンツデータを復号した後、それが表すコンテンツを再生し出力する。

【0007】以上のコンテンツ配信システムでは、権利管理技術としてのDRM(Digital Rights Management)

により、デジタルライツが保護されている。DRMによるデジタルライツの保護は、以下の3つの技術により実現される。第1の保護技術では、コンテンツ配信装置は、暗号化されたコンテンツデータと、端末固有情報で暗号化されたコンテンツ復号鍵を送信する。ここで、コンテンツ復号鍵は、コンテンツデータを要求したPC以外では復号できない。それゆえ、たとえ、暗号化されたコンテンツデータが他のPCに転送されたとしても、他のPCは、コンテンツ復号鍵の暗号を解くことができず、その結果、コンテンツデータを再生することができない。以上のことから、DRMでは、コンテンツ復号鍵は、唯一のPCに括り付けられると言える。これにより、デジタルライツが保護される。

【0008】第2の保護技術は耐タンバ技術である。つまり、PCには、各暗号を解くための復号プログラムが必要となるが、当該復号プログラムの解析は、上述の耐タンバ技術により防止される。これによっても、デジタルライツが保護される。

【0009】第3に、上述したように、従来のコンテンツ配信システムでは、コンテンツ配信装置は、利用条件データをPCに送信する。PCは、受信した利用条件データを管理する。そして、PCは、コンテンツデータの利用毎に、自身が管理する利用条件データが表す利用条件をチェックし、今回の利用が利用条件に台致していない場合には、それ以降の処理を行わない。これによっても、デジタルライツが保護される。

【0010】

【発明が解決しようとする課題】近年、セットトップボックス、テレビジョン受像機、音楽再生機およびゲーム機器に代表されるPC以外の民生機器にもネットワーク接続機能が付加されるようになってきた。これによって、民生機器が上述のコンテンツ配信装置からコンテンツデータを受信できるようになり、さらには、複数の民生機器の間でデータ通信ができるようになってきた。以上のことから、民生機器にも権利管理技術が組み込まれることが望まれる。しかしながら、上述のDRMのような権利管理技術を民生機器に組み込むことは、以下の問題点を想定できるため得策ではない。

【0011】第1に、コンテンツ復号鍵は、唯一のPCに括り付けられるため、PCおよび他の民生機器の利用者が同一であっても、他の民生機器は、そのコンテンツ復号鍵を使って、コンテンツデータを復号することができないという問題点があった。このような問題点ゆえ、利用者は、コンテンツデータを利用する際には、コンテンツ鍵を利用できるPCを使わなければならないため、従来の権利管理技術は、利用者にとって使い勝手の良いものではなかった。

【0012】第2に、上述のDRMには、耐タンバ技術が組み込まれ、さらに、PCがコンテンツデータを再生する前に必ず、内部に格納した利用条件データに基づい

て、当該コンテンツデータを利用可能か否かをチェックする。このように耐タンバ技術は上述のPCに大きな処理負担を強い。しかしながら、PCは、例えば、ビデオ再生、オーディオ再生またはゲームプレイ等、汎用的な用途に使えるよう、相対的に高性能なハードウェアを実装している。それゆえ、PCにDRMを組み込んで、さほど問題にはならない。それに対して、民生機器に求められるのは低価格であり、さらに、民生機器は、ビデオ再生、オーディオ再生およびゲームプレイのそれぞれに特化した用途に使用されることが一般的である。以上の観点から、民生機器には、PCほど高性能なハードウェアが実装されておらず、大きな処理負担を要求するDRMを組み込むのは困難であるという問題点があった。

【0013】それ故に、本発明の第1の目的は、複数の民生機器が共通のデジタルライツを共有できる権利管理技術を提供することである。また、本発明の第2の目的は、民生機器に適した権利管理技術を提供することである。

【0014】

【課題を解決するための手段および発明の効果】上記第1の目的を達成するために、本願の第1の発明は、複数の機器がコンテンツデータを利用するための権利を表す利用権情報を管理するための装置であって、複数の機器に割り当てられる利用権情報を含む利用権データベース（以下、利用権DBと称する）と、各機器からの発行要求に回答して、利用権DBに含まれる利用権情報を使って、発行要求を送信した機器に対するコンテンツデータの利用許可を示す利用許可情報を生成する利用権管理部と、利用権管理部で生成された利用許可情報を少なくとも含むライセンス情報を生成するライセンス情報生成部と、ライセンス情報生成部で生成されたライセンス情報を、発行要求を送信した機器に送信する通信部とを備える。

【0015】上記のように第1の発明によれば、利用権情報は、複数の機器に割り当てられるので、複数の機器が共通の利用権情報を共有可能な権利保護技術を提供することが可能となる。

【0016】上記第2の目的を達成するために、本願の第2の発明は、伝送路を通じて接続された利用権管理装置から、ライセンス情報の提供を受ける機器であって、可搬型記録媒体は、自身を一意に特定するメディア識別子を格納しており、機器は、可搬型記録媒体をデータ通信可能に接続するインターフェイスと、インターフェイスに接続された可搬型記録媒体からメディア識別子を取り出す識別子抽出部と、識別子抽出部から受け取るメディア識別子を使って、コンテンツデータの利用許可を受けるために必要な発行要求を生成する発行要求生成部と、発行要求生成部から受け取る発行要求を、伝送路を通じて、利用権管理装置に送信する第1の通信部とを備

える。ここで、利用権管理装置は、可搬型記録媒体に与えられたコンテンツデータの利用権情報を管理しており、機器からの発行要求にตอบสนองして、可搬型記録媒体が接続された機器におけるコンテンツデータの利用を制御するためのライセンス情報を生成して送信する。機器はさらに、利用権管理装置からのライセンス情報を処理して、コンテンツデータの利用を制御するライセンス情報処理部とを備える。

【0017】上記のように第2の発明によれば、コンテンツデータの利用権情報を利用権管理装置側で管理しているため、機器に、利用権情報のためにかかる処理負担を負わせる必要が無くなる。これによって、相対的に処理能力の低い機器に適した権利保護技術を提供することが可能となる。

【0018】さらに、第2の発明によれば、機器において、識別子抽出部は、機器に接続された可搬型記録媒体から、メディア識別子を取り出す。さらに、発行要求生成部は、取り出されたメディア識別子を使って発行要求を生成することができる。これによって、可搬型記録媒体のユーザは、自分の利用権情報を使って、他者の機器上でコンテンツデータを利用することが可能となる。

【0019】

【発明の実施の形態】「第1の実施形態」図1は、本発明の第1の実施形態に係る利用権管理装置11を収容したライセンス情報管理システムSaの全体構成を示すブロック図である。図1において、ライセンス情報管理システムSaは、利用権管理装置11と、複数の機器21の一例として2つの機器21aおよび21bと、伝送路31とを備えている。利用権管理装置11は、コンテンツ配信に関わる事業者α側に設置される。また、機器21aおよび21bは、典型的には、事業者αとの契約に基づいてコンテンツ配信を受ける契約者βにより使用される。また、伝送路31は、有線または無線であり、利用権管理装置11と、機器21aまたは機器21bとをデータ通信可能に接続する。

【0020】次に、図2を参照して、図1の利用権管理装置11の詳細な構成について説明する。図2において、利用権管理装置11は、コンテンツデータベース111と、復号鍵データベース112と、ユーザ情報データベース113と、利用権データベース114と、通信部115と、ユーザ認証部116と、利用権管理部117と、コンテンツ管理部118と、コンテンツ暗号化部119と、送信データ生成部120と、ライセンス情報生成部121と、復号鍵管理部122と、復号鍵暗号化部123とを備えている。また、ライセンス情報生成部121は、より詳しくは、図3に示すように、ハッシュ値生成部1211と、ライセンス情報組立部1212とを含んでいる。

【0021】次に、図4を参照して、図1の機器21aおよび21bの詳細な構成について説明する。図4にお

いて、機器21aおよび21bは、典型的には、パーソナルコンピュータ（以下、PCと称する）、セットトップボックス、音楽再生機、テレビジョン受像機およびゲーム機のいずれかである。ただし、本実施形態では、便宜上、機器21aおよび21bは、それぞれが音楽再生機能を有するPCおよび音楽再生機であると仮定する。この仮定下では、機器21aおよび21bのそれぞれは少なくとも、機器識別子格納部211と、設定要求生成部212と、通信部213と、コンテンツ管理部214と、コンテンツ蓄積部215と、発行要求生成部216と、ライセンス情報処理部217と、コンテンツ復号部218と、コンテンツ再生部219とを備えている。また、ライセンス情報処理部217は、より詳しくは、図5に示すように、改竄判定部2171と、ハッシュ値生成部2172と、利用許可判定部2173と、復号鍵復号部2174とを含んでいる。

【0022】次に、上記ライセンス情報管理システムSaにおいて、契約者βが事業者αからコンテンツ配信を受けるために必要となる準備について説明する。この準備作業では、図2のコンテンツデータベース（以下、コンテンツDBと称す）111と、復号鍵データベース（以下、復号鍵DBと称す）112と、ユーザ情報データベース（以下、ユーザ情報DBと称す）113とが事業者αにより構築される。

【0023】まず、図6(a)を参照して、図2のコンテンツDB111について詳細に説明する。まず、事業者αは、契約者βに配信されるコンテンツデータDcntを、自分で作成したり、別のコンテンツ制作者から受け取る。ここで、コンテンツデータDcntは、機器21aおよび21bの両方で利用可能なデータであって、例えば、テレビ番組、映画、ラジオ番組、音楽、書籍または印刷物を表す。また、コンテンツデータDcntは、ゲームプログラムまたはアプリケーションソフトウェアであっても良い。ただし、便宜上、本実施形態では、コンテンツデータDcntは音楽を表すデータであると仮定する。

【0024】事業者αは、以上のようにして得たコンテンツデータDcntのそれぞれに、コンテンツ識別子1cntを割り当てる。コンテンツ識別子1cntは好ましくは、本ライセンス情報管理システムSaにおいてコンテンツデータDcntを一意に特定する情報である。さらに、コンテンツ識別子1cntは、コンテンツデータDcntの格納場所を示すロケータでもあることが好ましい。また、以上のコンテンツデータDcntは、デジタルライツを保護する観点から、利用権管理装置11側で暗号化された状態で機器21aまたは21bに配信される。そのため、事業者αは、各コンテンツデータDcntに専用の暗号鍵Keを割り当てる。以上のコンテンツ識別子1cnt、コンテンツデータDcntおよび暗号鍵Keの組み合わせがコンテンツDB111に蓄積される。したがっ

て、図6(a)に示すように、コンテンツDB111は、コンテンツ識別子1cnt、コンテンツデータDcntおよび暗号鍵Keの組み合わせの集まりとなる。コンテンツDB111において、コンテンツ識別子1cntは特に、同じ組みのコンテンツデータDcntを一意に特定する。また、暗号鍵Keは、同じ組みのコンテンツデータDcntを暗号化するために使用される。

【0025】また、本実施形態では、図示の簡素化するため、コンテンツDB111は、コンテンツ識別子1cnt、コンテンツデータDcntおよび暗号鍵Keから構成され10とて説明するが、コンテンツデータDcntおよび暗号鍵Ke毎のデータベースが構築されてもよい。また、コンテンツ識別子1cntは、コンテンツデータDcntのロケータであることが好ましい。このような場合、利用権管理装置11は、機器21aまたは21bの設定要求Drraに含まれるコンテンツ識別子1cntを使って、コンテンツDB111からコンテンツデータDcntを読み出せるので、コンテンツDB111に、コンテンツ識別子1cntを登録しておく必然性はない。

【0026】次に、図6(b)を参照して、図2の復号鍵DB112について詳細に説明する。上述のように、各コンテンツデータDcntは暗号鍵Keで暗号化された状態で機器21aまたは21bに送信される。ここで、以下の説明では、暗号鍵Keで暗号化されたコンテンツデータDcntを、暗号済みコンテンツデータDecntと称する。暗号済みコンテンツデータDecntの復号のためには、暗号鍵Keに対応する復号鍵Kdが、機器21aまたは21bに提供される必要がある。この必要性から、事業者αは、コンテンツDB111内の各暗号鍵Keに対応する復号鍵Kdを準備する。ここで、復号鍵Kdは、暗号鍵Keと同じビット列からなっている15とよいし、異なるビット列からなっているもよい。以上の復号鍵Kdは、上述のコンテンツ識別子1cntと共に、復号鍵DB112に登録される。以上のことから、復号鍵DB112は、図6(b)に示すように、コンテンツ識別子1cntおよび復号鍵Kdの組み合わせの集まりとなる。復号鍵DB112において、コンテンツ識別子1cntは特に、同じ組みの復号鍵Kdに割り当てられているコンテンツデータDcntを特定する。また、復号鍵Kdは、同じ組みのコンテンツ識別子1cntで特定される暗号済みコンテンツデータDecntを復号するために使用される。

【0027】次に、図7(a)を参照して、図2のユーザ情報DB113について詳細に説明する。上述のように、契約者βは、事業者αとコンテンツ配信に係る契約を交わす。ここで、両者の契約に関しては、契約者βが伝送路31を通じて事業者αと行ってもよいし、他の形態で行ってもよい。この契約に基づいて、事業者αは、契約者βが所有する複数の機器21(つまり、機器21aおよび21b)のそれぞれに機器識別子1dvを割り当20

てる。ここで、図1に示すように、本実施形態では、機器21aと21bとが例示されているから、事業者αは、それぞれの機器識別子1dvとして機器識別子1dvaおよび1dvbを割り当てる。機器識別子1dvaおよび1dvbは、ライセンス情報管理システムSaにおいて、契約者β側の機器21aおよび21bを一意に特定する。以上の機器識別子1dvaおよび1dvbが、ユーザ情報DB113に登録される。さらに、事業者αは、契約者βおよびその関係者が、機器21aおよび21bのいずれを使っても、コンテンツデータDcntを利用できるように、グループ識別子1qpを、契約者βとの契約に割り当てる。ここで、契約者βおよびその関係者を包括的に述べるができるように、これらをユーザβと称する。以上の機器識別子1dvaおよび1dvbと、グループ識別子1qpとを使って、事業者αは、ユーザ情報DB113を構築する。

【0028】より具体的には、ユーザ情報DB113は、図7(a)に示すように、複数の契約者レコードRcsの集まりである。契約者レコードRcsは、1契約毎に作成され、典型的には、グループ識別子1qpと、機器識別子数Ndvと、複数の機器識別子1dvを含む。グループ識別子1qpは、契約者レコードRcsに含まれる複数の機器識別子1dvが同一のグループに属することを特定する。機器識別子数Ndvは、グループ識別子1qpで特定されるグループに属する機器21の数を示す。各機器識別子1dvは、グループ識別子1qpで特定されるグループに属する各機器21を特定する。以上の契約者レコードRcsにより、利用権管理装置11は、複数の機器21が同一グループに属することを把握することができる。なお、もし、契約者が1台の機器21しか使わない場合には、契約者レコードRcsは、それに割り当てられた機器識別子1dvのみを含んでいれば良い。

【0029】ここで図4を再度参照する。事業者αにより割り当てられた機器識別子1dvaおよび1dvbはさらに、ユーザβ側の機器21aおよび21bにおける機器識別子格納部211に設定される。ここで注意を要するのは、図4では機器識別子1dvaおよび1dvbの双方が機器識別子格納部211に格納されるように見えるが、そうではなく、機器21aの機器識別子格納部211には機器識別子1dvaが設定され、機器21bの機器識別子格納部211には機器識別子1dvbが設定される。また、以上の機器識別子1dvaおよび1dvbの設定に関しては、例えば、事業者αがユーザβ側の機器21aまたは21bを操作して設定する。また、他にも、事業者α側が、伝送路31を通じて、契約者βに割り当てた機器識別子1dvaまたは1dvbを機器21aまたは21bに送信し、それぞれが、受信した機器識別子1dvaまたは1dvbを、それぞれの機器識別子格納部211に自動的に設定するようにしてもよい。さらに、以上の機器識別子1dvaおよび1dvbは、機器21aまたは21bの工

場出荷時に、それぞれの機器識別子格納部211に設定されている。このような場合、契約者βは、契約時に、機器21aおよび21bに設定されている機器識別子1dvaおよび1dvbを事業者αに告知する。事業者αは、告知された機器識別子1dvaおよび1dvbを使って、ユーザ情報DB113を構築する。

【0030】また、図7(b)には、利用権データベース114が示されているが、これについては後述する。

【0031】以上の準備が終了すると、機器21aおよび21bの一方は、ユーザβの操作に従って、利用権管理装置11に対して、コンテンツデータDcntの利用権を設定することや、コンテンツデータDcntを取得することが可能となる。以下、図8を参照して、コンテンツデータDcntの利用権設定および取得時における、機器21aおよび利用権管理装置11の間のデータ通信について説明する。まず、ユーザβは、機器21aを操作して、利用権管理装置11にアクセスし、コンテンツDB111内のコンテンツデータDcntから、今回取得したいもののコンテンツ識別子1cntを特定する。以降の説明において、今回指定されたコンテンツデータDcntを、取得対象コンテンツデータDcntと称する。さらに、ユーザβは、取得対象コンテンツデータDcntを利用する際の利用条件Ccntを指定する。

【0032】以下、利用条件Ccntについて、より詳細に説明する。利用条件Ccntは、どのような条件で、機器21aがコンテンツデータDcntの利用権の設定を要求するのを示す情報である。コンテンツデータDcntが音楽を表す場合、利用条件Ccntとしては、有効期間、再生回数、最大連続再生時間、総再生時間または再生品質が代表的である。また、利用条件Ccntは、有効期間、再生回数、最大連続再生時間、総再生時間および再生品質の内、2つ以上の組み合わせであってもよい。利用条件Ccntとしての有効期間は、例えば、2001年6月1日から2001年8月31日までと設定され、設定された期間に限り、機器21aは、コンテンツデータDcntを再生できる。再生回数は、例えば、5回と設定され、設定された回数に限り、機器21aは、コンテンツデータDcntを再生できる。最大連続再生時間は、例えば、10秒と設定され、1回の再生において設定された時間までであれば、機器21aは、コンテンツデータDcntを再生できる。このような最大連続再生時間は、音楽のプロモーションに特に有効である。総再生時間は、例えば、10時間と設定され、設定された時間の範囲内であれば、機器21aは、コンテンツデータDcntを自由に再生できる。再生品質は、例えば、CD(Compact Disc)の品質と設定され、機器21aは、設定された再生品質でコンテンツデータDcntを再生できる。

【0033】なお、上述では、コンテンツデータDcntが音楽を表す場合に設定される利用条件Ccntについて説明した。しかし、上述のみに限らず、利用条件Ccnt

tは、コンテンツデータDcntが表す内容に応じて、適切に設定されることが好ましい。また、便宜上、本実施形態では、利用条件Ccntは、コンテンツデータDcntの再生回数であるとして、以下の説明を続ける。

【0034】上述したように、ユーザβは、機器21aを操作して、コンテンツ識別子1cntおよび利用条件Ccntを指定する。この指定に応答して、機器21aは、図9(a)に示す設定要求Drraを生成し、利用権管理装置11に送信する(図8;ステップS11)。設定要求Drraは、取得対象コンテンツデータDcntの利用権設定を利用権管理装置11に要求するための情報であるが、本実施形態ではさらに、取得対象コンテンツデータDcntの配信を利用権管理装置11に要求するための情報でもある。ステップS11をより具体的に説明すると、まず、設定要求生成部212(図4参照)は、ユーザβが指定したコンテンツ識別子1cntおよび利用条件Ccntを受け取る。また、設定要求生成部212は、機器識別子格納部211から機器識別子1dvaを受け取る。その後、設定要求生成部212は、以上の機器識別子1dva、コンテンツ識別子1cntおよび利用条件Ccntに、予め保持する設定要求識別子1rrを付加して、設定要求Drra(図9(a)参照)を生成する。ここで、設定要求識別子1rrは、利用権管理装置11が設定要求Drraを特定するために使用される。設定要求生成部212は、以上の設定要求Drraを通信部213に渡す。通信部213は、受け取った設定要求Drraを、伝送路31を通じて、利用権管理装置11に送信する。

【0035】利用権管理装置11(図2参照)において、通信部115は、伝送路31を通じて送信されてくる設定要求Drraを受信して、ユーザ認証部116に渡す。ユーザ認証部116は、設定要求Drraを受け取ると、その送信元の機器21aが契約ユーザβの物であるか否かを判定するためのユーザ認証処理を行う(図8;ステップS12)。より具体的には、ユーザ認証部116は、上述のユーザ情報DB113(図7(a)参照)にアクセスし、受け取った設定要求Drra内の機器識別子1dvaに一致するものが、当該ユーザ情報DB113に登録されているか否かを確認する。ユーザ認証部116は、ユーザ情報DB113に一致するものが登録されている場合に限り、今回設定要求Drraが、ユーザβの機器21aから送信されてきたものであると認証する。ユーザ認証部116は、以上のユーザ認証が終了すると、受け取った設定要求Drraを利用権管理部117に渡す。

【0036】なお、契約ユーザβ以外からの設定要求Drraを受け取った場合、ユーザ認証部116は、ユーザ認証に失敗する。この場合、ユーザ認証部116は、受信設定要求Drraを利用権管理部117に渡すことなく廃棄する。

【0037】利用権管理部117は、ユーザ認証部11

6からの受信情報に設定されている設定要求識別子Irrを判定することで、今回の受信情報が設定要求Drraであることを認識する。この認識結果に従って、利用権管理部117（図2参照）は、利用権データベース（以下、利用権DBと称する）114にアクセスして、利用権DB114への利用権登録処理を行う（ステップS13）。より具体的には、利用権管理部117は、受信設定要求Drraから機器識別子Idivaおよびコンテンツ識別子Icntを取り出して、これらを含む利用権レコードRrqtが利用権DB114（図7（b）参照）に登録されているか否かを判断する（ステップS131）。今、利用権DB114には対象となる利用権レコードRrqtが未登録であると仮定すると、利用権管理部117は、ステップS132を実行する。なお、ステップS131で利用権レコードRrqtが登録済の場合の動作については、機器21bの動作と共に説明するため、ここではその説明を省略する。

【0038】ステップS132において、利用権管理部117はまず、受信設定要求Drraから機器識別子Idiva、コンテンツ識別子Icntおよび利用条件Ccntを取り出した後、ユーザ情報DB113（図7（a）参照）にアクセスする。そして、利用権管理部117は、今回取り出した機器識別子Idivaを含む契約者レコードRcsから、グループ識別子Igpならびに全ての機器識別子IdivaおよびIdivbを取り出す（ステップS132）。次に、利用権管理部117は、受信設定要求Drraから取り出した機器識別子Idiva、コンテンツ識別子Icntおよび利用条件Ccntと、ユーザ情報DB113から得たグループ識別子Igpならびに機器識別子IdivaおよびIdivbとの組み合わせを、利用権レコードRrqtとして利用権DB114に登録する（ステップS133）。ここで、利用権管理部117は、設定要求Drra内の利用条件Ccntで機器21aが取得対象コンテンツデータDcntを利用する権利の付与を要求しているとみなす。以上のことから、利用権管理部117は、設定要求Drraから取り出した利用条件Ccntを利用権情報Drqtとして扱う。つまり、利用権情報Drqtは、利用条件Ccntが示す条件下で、コンテンツデータDcntを機器21aが利用する権利を示す。

【0039】以上の登録処理により、利用権DB114は、図7（b）に示すように、グループ識別子Igp、機器識別子IdivaおよびIdivb、コンテンツ識別子Icntならびに利用権情報Drqtを含む利用権レコードRrqtの集まりとなる。これによって、利用権管理部117は、契約者βの取得対象コンテンツデータDcnt毎に、その利用権を管理する。また、本実施形態の特徴の一つとして、利用権レコードRrqtに、ユーザ情報DB113から得た全ての機器識別子IdivaおよびIdivbを付加することで、機器21aからの設定要求Drraにより、機器21aおよび21bは、コンテンツデータDcntの利

用権を共有できるようになる。利用権管理部117は、以上の利用条件登録処理が終了すると、今回受け取った設定要求Drraをコンテンツ管理部118に渡す。

【0040】今回の設定要求Drraには、利用条件Ccntとして「再生m回」（mは自然数）が設定されていると仮定すると、図7（b）に示すように、今回新規登録される利用権レコードRrqtは、「再生m回」という条件が指定された利用権情報Drqtを含むことになる。

【0041】なお、本ライセンス情報管理システムSaの技術的特徴とは関係ないが、ステップS13において、利用権管理部117は、利用条件情報Dcntの登録毎に、機器識別子Idivaが割り当てられている契約者βに、コンテンツデータDcntの利用に対する課金を行ってもよい。

【0042】コンテンツ管理部118は、設定要求Drraを受け取ると、コンテンツデータDcntおよびそれ専用の暗号鍵Keの読み出し処理を行う（ステップS14）。より具体的には、コンテンツ管理部118は、受信設定要求Drraから、コンテンツ識別子Icntを取り出す。その後、コンテンツ管理部118は、コンテンツDB111にアクセスして、取り出したコンテンツ識別子Icntが割り当てられているコンテンツデータDcntおよび暗号鍵Keを読み出す。以上の読み出し処理が終了すると、コンテンツ管理部118は、読み出したコンテンツデータDcntおよび暗号鍵Keをコンテンツ暗号化部119に渡す。さらに、コンテンツ管理部118は、受け取った設定要求Drraを送信データ生成部120に渡す。

【0043】コンテンツ暗号化部119は、コンテンツデータDcntの暗号処理を行う（ステップS15）。より具体的には、コンテンツ暗号化部119は、受け取ったコンテンツデータDcntを、同時に受け取った暗号鍵Keで暗号化して、前述の暗号済みコンテンツデータDecntを生成する。コンテンツ暗号化部119は、以上の暗号処理が終了すると、暗号済みコンテンツデータDecntを送信データ生成部120に渡す。

【0044】送信データ生成部120は、コンテンツ管理部118からの設定要求Drraと、コンテンツ暗号化部119からの暗号済みコンテンツデータDecntとが揃うと、送信データ生成処理を行う（ステップS16）。より具体的には、送信データ生成部120は、受信設定要求Drraから、コンテンツ識別子Icntおよび機器識別子Idivaを取り出す。さらに、送信データ生成部120は、取り出した機器識別子Idivaおよびコンテンツ識別子Icntを、受け取った暗号済みコンテンツデータDecntに付加して、図9（b）に示すような、送信データDtrnaを生成する。送信データ生成部120は、以上の送信データ生成処理が終了すると、送信データDtrnaを通信部115に渡す。通信部115は、受け取った送信データDtrnaを、伝送路31を介して、機器21aへと

送信する(ステップS17)。

【0045】機器21a(図4参照)において、通信部213は、伝送路31を通じて送信されてくる送信データDtmaを受信する(ステップS18)。より具体的には、通信部213は、それに含まれる機器識別子I dvaとコンテンツ識別子I cntとから、今回、取得対象コンテンツデータDcntを含む自分宛の送信データDtmaを受信したことを認識する。このような認識結果に従って、通信部213は、受信データDtmaをコンテンツ管理部214に渡す。

【0046】コンテンツ管理部214は、受信データDtma内のコンテンツ識別子I cntおよび暗号済みコンテンツデータDecntを、コンテンツ蓄積部215に蓄積する(ステップS19)。つまり、コンテンツ蓄積部215には、図10に示すように、上述の設定要求Drraを使って要求したコンテンツ識別子I cntおよび暗号済みコンテンツデータDecntの組みが、いくつか蓄積されることになる。

【0047】デジタルライツの保護の観点から、機器21aには暗号済みコンテンツデータDecntが配信される。そのため、機器21aは、コンテンツデータDcntを利用する場合には、利用権管理装置11により提供される復号鍵Kdで、暗号済みコンテンツデータDecntを復号する必要がある。ここで、本ライセンス情報管理システムSaでは、復号鍵Kdを機器21aに提供するために、ライセンス情報Dlcaが用いられる。以下、図11～図13を参照して、ライセンス情報Dlcaの取得およびコンテンツデータDcntの復号時における機器21aおよび利用権管理装置11の動作について説明する。

【0048】まず、ユーザβは、機器21aを操作して、コンテンツ蓄積部215に蓄積されている暗号済みコンテンツデータDecntの中から、今回利用したいものを特定する。ここで、以下の説明において、今回指定された暗号済みコンテンツデータDecntを、復号対象コンテンツデータDecntと称する。ユーザβによる指定に回答して、機器21aは、図14(a)に示すような発行要求Diraを生成し、利用権管理装置11に送信する

(図11;ステップS21)。発行要求Diraは、上述のライセンス情報Dlcaの発行を利用権管理装置11に機器21aが要求するための情報である。より具体的には、コンテンツ管理部214(図4参照)は、契約者βにより特定された復号対象コンテンツデータDecntに付加されているコンテンツ識別子I cntを、コンテンツ蓄積部215から取り出して、発行要求生成部216に渡す。発行要求生成部216は、コンテンツ管理部214により取り出されたコンテンツ識別子I cntを受け取る。さらに、発行要求生成部216は、機器識別子格納部211から機器識別子I dvaを取り出す。その後、発行要求生成部216は、機器識別子I dvaおよびコンテンツ識別子I cntの組み合わせに、発行要求識別子I ir

を付加して、発行要求Dira(図14(a)参照)を生成する。ここで、発行要求識別子I irは、利用権管理装置11が発行要求Diraを特定するために使用される。発行要求生成部216は、以上の発行要求Diraを通信部213に渡す。通信部213は、受け取った発行要求Diraを伝送路31を通じて、利用権管理装置11に送信する。

【0049】利用権管理装置11において、通信部115(図2参照)は、伝送路31を通じて送信されてくる発行要求Diraを受信して、ユーザ認証部116に渡す。ユーザ認証部116は、発行要求Diraを受け取ると、ユーザ認証処理を行う(ステップS22)。ステップS22におけるユーザ認証は、ステップS12のそれと同様であるため、詳細な説明を省略する。ユーザ認証部116は、ユーザ認証に成功した場合に限り、受信発行要求Diraを利用権管理部117に渡す。

【0050】利用権管理部117は、それに設定されている発行要求識別子I irを確認して、ユーザ認証部116から渡されたものが発行要求Diraであることを認識する。この認識結果に従って、利用権管理部117は、受け取った発行要求Diraから、機器識別子I dvaおよびコンテンツ識別子I cntを取り出す(ステップS23)。次に、利用権管理部117は、取り出した機器識別子I dvaおよびコンテンツ識別子I cntの組み合わせと同じものを含む利用権レコードRrqtが、利用権DB114(図7(b)参照)に登録されているか否かを判断する(ステップS24)。

【0051】利用権管理部117は、ステップS24で「Yes」と判断した場合、対象となる利用権レコードRrqtに含まれる利用権情報Drqtを参照して、機器21aに利用許可を与えることができるか否か、つまりコンテンツデータDcntの利用権が残っているか否かを判断する(ステップS25)。ステップS25で「Yes」と判断した場合、利用権管理部117は、対象となる利用権情報Drqtを参照して、利用許可情報Dlwaを生成する(ステップS26)。利用許可情報Dlwaは、復号対象コンテンツデータDecntの復号許可を機器21aに与えるための情報である。また、利用許可情報Dlwaの生成により、機器21aの利用権情報Drqtが使われることになるので、ステップS26の次に、利用権管理部117は、ステップS26で使われた分だけ利用権情報Drqtを更新する(ステップS27)。なお、ステップS27の実行時点で、全ての利用権情報Drqtが使われた場合には、それを含んでいた利用権レコードRrqtを利用権DB114から削除しても良い。

【0052】ここで、以上のステップS25～S27の処理の具体例について説明する。上述の仮定に従えば、今回対象となる利用権レコードRrqtにおいて、利用権情報Drqtは、図7(b)に示すように、「再生m回」という利用権を表す。したがって、ステップS25にお

いて、利用権管理部117は、機器21aに対し、復号対象コンテンツデータDecntの再生許可を与えてもよいと判断する。この判断に従って、利用権管理部117は、ステップS26で、利用許可情報Dlwaを作成する。この時生成される利用許可情報Dlwaとしては、例えば、「再生n回」が挙げられる。ここで、nは、上述のmを超えない自然数であり、例えば、ユーザBが機器21aを操作して指定した値である。他にも、nは、機器21aの処理能力に応じて、利用権管理部117側で設定しても良い。また、ステップS26により、機器21aが復号対象コンテンツデータDecntを再生する権利をn回使うことになる。そのため、ステップS27において、利用権管理部117は、利用権情報Drqtを「再生m回」から「再生(m-n)回」に更新する。

【0053】以上の具体例では、利用権情報DrqtがコンテンツデータDecntの再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムSaでは、様々な利用権情報Drqt（つまり利用条件Cnt）を設定することができる。従って、ステップS23からS27までの処理手順は、利用権情報Drqtに応じて適切に規定される必要がある。

【0054】以上の利用許可情報Dlwaを、利用権管理部117（図2参照）は、発行要求Diraと一緒に、ライセンス情報生成部121に渡す。より具体的には、ライセンス情報生成部121は、図3に示すように、ハッシュ値生成部1211およびライセンス情報組立部1212を含んでいる。ハッシュ値生成部1211には、利用許可情報Dlwaのみが渡され、また、ライセンス情報組立部1212には、利用許可情報Dlwaおよび発行要求Diraの双方が渡される。

【0055】まず、ハッシュ値生成部1211は、予め保持するハッシュ関数 $f(x)$ に、受け取った利用許可情報Dlwaを代入して、利用許可情報Dlwaの改竄を防止するためのハッシュ値Vhsaを生成する（ステップS28）。つまり、ハッシュ値Vhsaは、利用許可情報Dlwaを生成多項式 $f(x)$ に代入した時に得られる解である。以上のようなハッシュ値Vhsaを、ハッシュ値生成部1211は、ライセンス情報組立部1212に渡す。

【0056】ライセンス情報組立部1212は、受け取った発行要求Diraを復号鍵管理部122に渡す。復号鍵管理部122（図2参照）は、前述した復号鍵DB112（図6（b）参照）を管理する。復号鍵管理部122は、受け取った発行要求Diraに設定されているコンテンツ識別子Icntおよび機器識別子Idvaを取り出す。さらに、復号鍵管理部122は、コンテンツ識別子Icntと同じ組みの復号鍵Kdを復号鍵DB112から取り出して、機器識別子Idvaと一緒に復号鍵暗号化部123に渡す。復号鍵暗号化部123は、受け取った復号鍵Kdを、同時に受け取った機器識別子Idvaを使

て暗号化して（ステップS29）、暗号済みの復号鍵Kedaを生成する。以上の暗号済み復号鍵Kedaおよび機器識別子Idvaは、ライセンス情報組立部1212に渡される。

【0057】ライセンス情報組立部1212は、発行要求Diraおよび利用許可情報Dlwa、ハッシュ値Vhsaならびに暗号済み復号鍵Kedaのすべてが揃うと、図14（b）に示すライセンス情報Dlcaの生成を開始する（図12：ステップS210）。より具体的には、ライセンス情報組立部1212は、発行要求Diraから、コンテンツ識別子Icntおよび機器識別子Idvaを取り出して、それぞれを、利用許可情報Dlwa、暗号済み復号鍵Kedaおよびハッシュ値Vhsaの組み合わせに付加する。さらに、ライセンス情報組立部1212は、予め保持するライセンス情報識別子Ilcを、機器識別子Idvaに付加して、ライセンス情報Dlcaを生成する。以上のライセンス情報Dlcaは、復号対象コンテンツデータDecntの機器21aにおける利用を制御するための情報である。また、ライセンス情報識別子Ilcは、機器21aがライセンス情報Dlcaを特定するための情報である。また、以上のライセンス情報Dlcaは、通信部115および伝送路31を通じて、機器21aに送信される（ステップS211）。

【0058】機器21a（図4参照）において、通信部213は、伝送路31を通じて送信されてくるライセンス情報Dlcaを受信する（ステップS212）。より具体的には、通信部213は、受信情報に含まれる機器識別子Idvaから、自分宛の情報が到着したと判断し、さらに、それに設定されるライセンス情報識別子Ilcから、今回、ライセンス情報Dlcaを受け取ったことを認識する。このような認識結果に従って、通信部213は、受け取ったライセンス情報Dlcaをライセンス情報処理部217に渡す。

【0059】ライセンス情報処理部217は、図5に示すように、改竄判定部2171と、ハッシュ値生成部2172と、利用許可判定部2173と、復号鍵復号部2174とを含んでいる。通信部213からのライセンス情報Dlcaは、まず、改竄判定部2171に渡される。改竄判定部2171は、まず、受け取ったライセンス情報Dlcaから、利用許可情報Dlwaおよびハッシュ値Vhsaを取り出し（ステップS213）、取り出した利用許可情報Dlwaを、ハッシュ値生成部2172に渡し、ハッシュ値Vhsaをそのまま保持する。ここで、以下の説明において混同が生じないように、ステップS213で取り出されたハッシュ値Vhsaを、機器21aの外部（つまり利用権管理装置11）で生成されたものであるという観点から、外部ハッシュ値Vehsaと称する。

【0060】ハッシュ値生成部2172は、利用権管理装置11側のハッシュ値生成部1211（図3参照）と同じハッシュ関数 $f(x)$ を保持しており、受け取った

利用許可情報D1waをハッシュ関数f(x)に代入してハッシュ値Vhsaを生成する(ステップS214)。ここでステップS214で生成されたハッシュ値Vhsaを、機器21aの内部で生成されたものであるという観点から、内部ハッシュ値V1hsaと称する。ハッシュ値生成部2172は、以上の内部ハッシュ値V1hsaを、改竄判定部2171に返す。

【0061】改竄判定部2171は、上述の内部ハッシュ値V1hsaを受け取ると、利用許可情報D1waが改竄されているか否かを判定する(ステップS215)。より具体的には、上述の内部ハッシュ値V1hsaは、ライセンス情報D1ca内の利用許可情報D1waが改竄されていないという条件で、外部ハッシュ値Vehsaに一致する。そこで、ステップS215において、改竄判定部2171は、受け取った内部ハッシュ値V1hsaが外部ハッシュ値Vehsaに一致するか否かを判定する。改竄判定部2171は、「Yes」と判定した場合には、利用許可情報D1waが改竄されておらず、今回送信されてきた利用許可情報D1waが有効であるとみなして、今回受け取ったライセンス情報D1caを利用許可判定部2173に渡す。【0062】利用許可判定部2173は、受け取ったライセンス情報D1caを参照して、復号対象コンテンツデータDecntの利用が許可されているか否かを判定する(ステップS216)。利用許可判定部2173は、ステップS216において「Yes」と判断した場合に限り、受け取ったライセンス情報D1caから、暗号済み復号鍵Kedaを取り出して、復号鍵番号部2174に渡す。

【0063】ここで、以上のステップS216の処理の具体例について説明する。前述の仮定に従えば、今回のライセンス情報D1caの利用許可情報D1waにより、コンテンツデータDcntの再生がn回だけ許可されている。かかる場合、利用許可判定部2173は、ステップS216において、利用許可情報D1waに設定される再生回数が1以上であれば、復号対象コンテンツデータDecntの利用が許可されていると判断して、受け取ったライセンス情報D1caを復号鍵番号部2174に渡す。

【0064】以上の具体例では、利用権情報DrqtがコンテンツデータDcntの再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムSaでは、様々な利用権情報Drqt(つまり利用条件Cnt)を設定することができる。従って、ステップS216の処理は、利用権情報Drqtに応じて適切に規定される必要がある。

【0065】復号鍵番号部2174は、利用許可判定部2173から暗号済み復号鍵Kedaを受け取る。さらに、復号鍵番号部2174は、機器識別子格納部211から機器識別子Idvaを取り出す。その後、復号鍵番号部2174は、暗号済み復号鍵Kedaを、機器識別子Idvaで復号して(ステップS217)、復号鍵Kdをコ

ンテンツ復号部218に渡す。

【0066】ところで、コンテンツ管理部214は、以上のステップS217の次またはそれ以前に(図12にはステップS217の直後の例が示されている)、今回の復号対象コンテンツデータDecntをコンテンツ蓄積部215から取り出す(ステップS218)。取り出された復号対象コンテンツデータDecntは、コンテンツ復号部218に渡される。コンテンツ復号部218は、復号鍵番号部2174から受け取った復号鍵Kdで、復号対象コンテンツデータDecntを復号して(ステップS219)、コンテンツデータDcntをコンテンツ再生部219に渡す。コンテンツ再生部219は、受け取ったコンテンツデータDcntを再生して、音声出力する(ステップS220)。これにより、契約者βは、事業者αから購入したコンテンツデータDcntが表す音楽を聴くことができる。

【0067】ここで、図12のステップS215を参照する。ステップS215において、改竄判定部2171は、利用許可情報D1waが改竄されていると判定する場合がある。また、ステップS216において、利用許可判定部2173は、復号対象コンテンツデータDecntの利用が許可されていないと判定する場合もある。このような場合、改竄判定部2171および利用許可判定部2173は、今回受け取ったライセンス情報D1caを破棄する(図13;ステップS221)。以上から明らかなように、本ライセンス情報管理システムSaでは、有効なライセンス情報D1caを受信した場合にのみ、復号対象コンテンツデータDecntの復号が許可される。これによって、上述のデジタルライツが保護される。

【0068】また、図11のステップS24において、利用権管理部117は、利用権レコードRrqtが利用権DB114(図7(b)参照)に登録されていないと判断する場合がある。さらに、ステップS25において、利用権管理部117は、機器21aに利用許可を与えることができないと判断する場合もある。このような場合、利用権管理部117は、復号対象コンテンツデータDecntの利用を拒否することを示す利用拒否情報Drj(図14(c)参照)を生成して、通信部115に渡す。通信部115は、受け取った利用拒否情報Drjを、伝送路31を介して、機器21aに送信する(図13;ステップS222)。

【0069】機器21a(図4参照)において、通信部213は、伝送路31を通じて送信されてくる利用拒否情報Drjを受信する(ステップS223)。利用拒否情報Drjの受信以降、機器21aでは何の処理も行われな。以上から明らかなように、本ライセンス情報管理システムSaでは、利用権DB114に有効な利用権レコードRrqtが登録されてない場合には、利用拒否情報Drjが、発行要求Diraの送信元となる機器21aに送信される。これによって、機器21a側では、復号対象コ

ンテンツデータ Decnt は復号されない。これによって、上述のデジタルライツが保護される。

【0070】なお、ステップ S 24 において、利用権管理部 117 は、利用権レコード R rqt が利用権 DB 114 (図 7 (b) 参照) に登録されていないと判断した後、利用権レコード R rqt を新たに生成して、利用権 DB 114 に登録するようにしてもよい。

【0071】次に、以上の利用権レコード R rqt の登録により、コンテンツデータ D cnt の利用権を機器 21a と共有している機器 21b および利用権管理装置 11 10 間のデータ通信、およびそれに関連するそれぞれの動作について説明する。なお、以下の機器 21b の動作は、上述の機器 21a の動作とほとんどの部分で同様であるから、その動作説明を簡素化する。まず、ユーザは、機器 21b を操作して、コンテンツ識別子 I cnt および利用条件 C cnt を指定する。この指定に応答して、機器 21b は、設定要求 D rrb を生成し、利用権管理装置 11 に送信する (図 8 ; ステップ S 11)。設定要求 D rrb は、設定要求 D rra と比較すると、機器識別子 I dva の代わりに、機器 21b を一意に特定する機器識別子 I 20 d vb を含む点で相違するだけであるから、その詳細な説明を省略する。なお、機器 21b は、自身が利用可能な利用権レコード R rqt が利用権 DB 114 に登録されていることが予め分かっている場合には、利用条件 C cnt を含まない設定要求 D rrb を生成しても良い。

【0072】利用権管理装置 11 (図 2 参照) において、ユーザ認証部 116 は、通信部 115 を通じて、機器 21b からの設定要求 D rrb を受け取る。その後、ユーザ認証部 116 は、機器 21b が契約ユーザの物であるか否かを判定するためのユーザ認証処理を行う (ステップ S 12)。ユーザ認証部 116 は、ユーザ認証処理が成功した場合に限り、受け取った設定要求 D rrb を利用権管理部 117 に渡す。

【0073】利用権管理部 117 は、今回の受信情報が設定要求 D rrb であることを認識すると、ステップ S 13 を行う。ステップ S 13 において、まず、利用権管理部 117 は、受信設定要求 D rrb 内の機器識別子 I d vb およびコンテンツ識別子 I cnt を含む利用権レコード R rqt が利用権 DB 114 (図 7 (b) 参照) に登録されているか否かを判断する (ステップ S 131)。前述したように、利用権 DB 114 には、機器 21a の設定要求 D rra に起因して、機器識別子 I d vb およびコンテンツ識別子 I cnt を含む利用権レコード R rqt が登録済である。この場合、利用権管理部 117 は、ステップ S 132 ~ S 133 を行うことなく、今回の設定要求 D rrb をコンテンツ管理部 118 に渡す。

【0074】コンテンツ管理部 118 は、設定要求 D rrb の受信後、コンテンツデータ D cnt および暗号鍵 Ke を読み出して (ステップ S 14)、それらをコンテンツ暗号化部 119 に渡す。さらに、コンテンツ管理部 11

8 は、受信設定要求 D rrb を送信データ生成部 120 に渡す。コンテンツ暗号化部 119 は、コンテンツデータ D cnt の暗号処理を行い (ステップ S 15)、それが終了すると、暗号済みコンテンツデータ Decnt と受信設定要求 D rrb とを送信データ生成部 120 に渡す。

【0075】送信データ生成部 120 は、前述したようにして、送信データ D trnb (図 9 (b) 参照) を生成する (ステップ S 16)。送信データ D trnb は、送信データ D trma と比較すると、機器識別子 I dva の代わりに、機器識別子 I d vb を含む点で相違するだけであるから、その詳細な説明を省略する。ステップ S 16 の次に、送信データ生成部 120 は、送信データ D trnb を通信部 115 に渡し、通信部 115 は、前述したように、受け取った送信データ D trnb を機器 21b へと送信する (ステップ S 17)。

【0076】機器 21b (図 4 参照) において、通信部 213 は、送信データ D trnb を受信し (ステップ S 18)、その後、受信データ D trnb をコンテンツ管理部 214 に渡す。コンテンツ管理部 214 は、受信データ D trnb 内のコンテンツ識別子 I cnt および暗号済みコンテンツデータ Decnt を、コンテンツ蓄積部 215 に蓄積する (ステップ S 19)。

【0077】デジタルライツの保護の観点から、機器 21b は、機器 21a の場合と同様に、利用権管理装置 11 からライセンス情報 D lcb の発行を受けなければ、コンテンツデータ D cnt を利用することができない。以下、図 11 ~ 図 13 を参照して、ライセンス情報 D lcb の取得およびコンテンツデータ D cnt の復号時における機器 21b および利用権管理装置 11 の動作について説明する。なお、この時の動作は、機器 21a および利用権管理装置 11 の動作とほとんどの部分で同様であるから、その動作説明を簡素化する。

【0078】まず、ユーザは、機器 21b を操作して、コンテンツ蓄積部 215 の中から、復号対象コンテンツデータ Decnt を指定する。ユーザの指定に答えて、機器 21b において、発行要求生成部 216 は、発行要求 D irb (図 14 (a) 参照) を生成し、利用権管理装置 11 に送信する (図 11 ; ステップ S 21)。発行要求 D irb は、発行要求 D ira と比較すると、機器識別子 I dva が機器識別子 I d vb に代わる点で相違するだけであるから、その詳細な説明を省略する。発行要求生成部 216 は、以上の発行要求 D irb を通信部 213 に渡す。通信部 213 は、受信発行要求 D irb を利用権管理装置 11 に送信する。

【0079】利用権管理装置 11 において、ユーザ認証部 116 (図 2 参照) は、通信部 115 を通じて、機器 21b が送信した発行要求 D irb を受け取り、その後、ユーザ認証処理を行う (ステップ S 22)。ユーザ認証部 116 は、ユーザ認証処理が成功した場合に限り、受信発行要求 D irb を利用権管理部 117 に渡す。利用権

管理部117は、受信発行要求Dirbから、機器識別子Idivおよびコンテンツ識別子Icntを取り出し（ステップS23）、その後、取り出した機器識別子Idivおよびコンテンツ識別子Icntの組み合わせと同じものを含む利用権レコードRratが、利用権DB114（図7（b）参照）に登録されているか否かを判断する（ステップS24）。

【0080】利用権管理部117は、ステップS24で「Yes」と判断した場合、対象となる利用権レコードRratに含まれる利用権情報Dratを参照して、機器21bに利用許可を与えることができるか否か、つまりコンテンツデータDcntの利用権が残っているか否かを判断する（ステップS25）。ステップS25で「Yes」と判断した場合、利用権管理部117は、対象となる利用権情報Dratを使って利用許可情報Dlwbを生成する（ステップS26）。利用許可情報Dlwbは、利用許可情報Dlwaと比較すると、機器識別子Idvaが機器識別子Idivに代わる点でのみ相違するから、その詳細な説明を省略する。ステップS26の次に、利用権管理部117は、ステップS26で使われた分だけ利用権情報Dratを更新する（ステップS27）。

【0081】以上の利用許可情報Dlwbを、利用権管理部117（図2参照）は、発行要求Dirbと一緒に、ライセンス情報生成部121に渡す。ライセンス情報生成部121において、ハッシュ値生成部1211（図3参照）は、予め保持するハッシュ関数f(x)に、受け取った利用許可情報Dlwbを代入して、利用許可情報Dlwbの改竄を防止するためのハッシュ値Vhsbを生成し（ステップS28）、それをライセンス情報組立部1212に渡す。

【0082】ライセンス情報組立部1212は、受け取った発行要求Dirbを復号鍵管理部122に渡す。復号鍵管理部122（図2参照）は、前述した復号鍵DB112（図6（b）参照）を管理しており、受信発行要求Dirbからコンテンツ識別子Icntおよび機器識別子Idivを取り出す。さらに、復号鍵管理部122は、コンテンツ識別子Icntと同じ組みの復号鍵Kdを復号鍵DB112から取り出して、機器識別子Idivと一緒に復号鍵暗号化部123に渡す。復号鍵暗号化部123は、受け取った復号鍵Kdを、同時に受け取った機器識別子Idivを使って暗号化して（ステップS29）、暗号済み復号鍵Kedbを生成する。以上の暗号済み復号鍵Kedbおよび機器識別子Idivは、ライセンス情報組立部1212に渡される。

【0083】ライセンス情報組立部1212は、発行要求Dirbおよび利用許可情報Dlwb、ハッシュ値Vhsbならびに暗号済み復号鍵Kedbのすべてが揃うと、ライセンス情報Dlcb（図14（b）参照）を生成する（図12；ステップS210）。ライセンス情報Dlcbは、ライセンス情報Dlcaと比較すると、機器識別子Idva

、利用許可情報Dlwa、暗号済み復号鍵Kedbおよびハッシュ値Vhsaが機器識別子Idiv、利用許可情報Dlwb、暗号済み復号鍵Kedbおよびハッシュ値Vhsbに代わる点で相違するだけであるから、その詳細な説明を省略する。以上のライセンス情報Dlcbは、通信部115および伝送路31を通じて、機器21bに送信される（ステップS211）。

【0084】機器21b（図4参照）において、通信部213は、伝送路31を通じて送信されてくるライセンス情報Dlcbを受信し（ステップS212）、それをライセンス情報処理部217に渡す。ライセンス情報処理部217において、改竄判定部2171は、受信ライセンス情報Dlcbから、利用許可情報Dlwbおよびハッシュ値Vhsbを取り出し（ステップS213）、取り出した利用許可情報Dlwbを、ハッシュ値生成部2172に渡し、ハッシュ値Vhsbを外部ハッシュ値Vehsbとして保持する。ハッシュ値生成部2172は、利用権管理装置11側と同じハッシュ関数f(x)を保持しており、受け取った利用許可情報Dlwbをハッシュ関数f(x)に代入して、内部ハッシュ値Vlhsbを生成し（ステップS214）、それを改竄判定部2171に返す。

【0085】改竄判定部2171は、前述と同様にし、上述の内部ハッシュ値Vlhsbを受け取ると、それが外部ハッシュ値Vehsbに一致するか否かを判定し（ステップS215）。両者が一致する場合には、今回の利用許可情報Dlwbが有効であるとして、受信ライセンス情報Dlcbを利用許可判定部2173に渡す。利用許可判定部2173は、前述と同様にし、復号対象コンテンツデータDecntの利用が許可されているか否かを判定し（ステップS216）、「Yes」と判断した場合に限り、受け取ったライセンス情報Dlcbから、暗号済み復号鍵Kedbを取り出して、復号鍵復号部2174に渡す。復号鍵復号部2174は、利用許可判定部2173から暗号済み復号鍵Kedbを受け取る。さらに、復号鍵復号部2174は、機器識別子格納部211から機器識別子Idivを取り出す。その後、復号鍵復号部2174は、暗号済み復号鍵Kedbを、機器識別子Idivで復号して（ステップS217）、その結果得られる復号鍵Kdをコンテンツ復号部218に渡す。

【0086】コンテンツ管理部214は、今回の復号対象コンテンツデータDecntをコンテンツ蓄積部215から取り出し（ステップS218）、それをコンテンツ復号部218に渡す。コンテンツ復号部218は、復号鍵復号部2174からの復号鍵Kdで、復号対象コンテンツデータDecntを復号して（ステップS219）、コンテンツデータDcntをコンテンツ再生部219に渡す。コンテンツ再生部219は、受け取ったコンテンツデータDcntを再生して、音声出力する（ステップS220）。

【0087】以上のように本実施形態によれば、利用権

レコード Rrqt には、複数の機器識別子 I dva および I dvb が記録される。これによって、利用権管理装置 11 は、互いに異なる機器 21a および 21b から発行要求 Dira および Dirb が送信されてきたとしても、利用権レコード Rrqt を参照することで、同一の利用権情報 D rqt から生成されたライセンス情報 D lca および D lcb をそれらに提供することができるようになる。以上の本実施形態によって、複数の機器が共通のデジタルライツを共有できる権利管理技術を提供することができる。

【0088】なお、以上の実施形態では、利用権レコード R rqt はグループ識別子 I qpを含んでいたが、これは、機器 21a および 21b が同一グループに属することを明確にするためのものである。つまり、グループ識別子 I qpは、利用権レコード R rqt に必須の情報ではない。また、利用権レコード R rqt は、機器 21a および 21b の機器識別子 I dva および I dvb を含まずに、グループ識別子 I qpのみを使って、同一グループに属する機器 21a および 21b を特定するようにしても良い。

【0089】また、以上の実施形態では、複数の機器 21の代表例として、2台の機器 21a および機器 21b を挙げたが、これに限らず、3台以上の機器で、同一の利用権情報 D rqt を共有するようにしても良い。

【0090】また、以上の実施形態では、図示の部台上、利用権管理装置 11がコンテンツ DB 111を備えると説明したが、これに限らず、コンテンツデータ D cnt は別のサーバから機器 21a および 21b に配信されても良い。

【0091】また、以上の実施形態では、ユーザ情報 DB 113に契約時に登録された機器 21a および 21b が同一の利用権情報 D rqt を共有する例について説明した。しかし、ユーザ側の機器 21は、必ずしも機器 21a および 21b の2台だけでコンテンツ配信を受けるわけではなく、新しく入手した機器 21を使ってコンテンツデータ D cnt を利用したい場合もある。以下に説明する利用権管理装置 11a ~ 11d は、上述の利用権管理装置 11の第1~第4の変型例であって、上述のニーズに対応するために提供される。「第1の変型例」

【0092】図15は、利用権管理装置 11a を収容したライセンス情報管理システム Sa1の全体構成を示すブロック図である。図15のライセンス情報管理システム Sa1は、図1のライセンス情報管理システム Saと比較すると、利用権管理装置 11に代えて利用権管理装置 11aを備えている点と、機器 21cをさらに備えている点で相違する。それ以外に両ライセンス情報管理システム Sa および Sa1に相違点はないので、図15において、図1の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。なお、図15には、通信ケーブル 32が示されているが、これは第4の変型例で使われる構成であるため、本変型例だけでなく、第2および第3の変型例では、通信ケーブル 32の説明を省

略する。

【0093】利用権管理装置 11a は、上述の事業者 α側に設置され、図2の利用権管理装置 11と比較すると、図16に示すように、ユーザ情報管理部 124と、登録完了生成部 125とをさらに備える点で相違する。それ以外に両利用権管理装置 11および 11aの間に相違点はない。それ故、図16において、図2の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【0094】機器 21c は、上述のユーザ βにより所有されるが、現時点では、利用権管理装置 11aのユーザ情報 DB 113に未登録の機器であって、図4の機器 21aまたは 21bと比較すると、図17に示すように、登録要求生成部 220およびグループ識別子格納部 221をさらに備える点で相違する。それ以外に、両機器 21a および 21b と、機器 21cとの間には相違点はない。それ故、図17において、図4の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。なお、機器 21cの機器識別子格納部 211には、機器 21cを一意に特定するための機器識別子 I dvcが予め格納されており、グループ情報格納部 221には、ユーザ βに割り当てられたグループ識別子 I qpが格納されていると仮定する。

【0095】次に、図18を参照して、以上のような構成のライセンス情報管理システム Sa1において、機器 21cをユーザ情報 DB 113に登録するまでの機器 21c および利用権管理装置 11aの動作について説明する。まず、機器 21cは、ユーザ βの操作に従って、ユーザ βが事業者 αから通知されるグループ識別子 I qpを、グループ識別子格納部 221に格納する。その後、ユーザ βは、機器 21cを操作して、本機器 21cをユーザ情報 DB 113に登録する旨を指定する。この指定に応答して、機器 21cにおいて、登録要求生成部 220は、図19(a)に示す登録要求 Drscを生成し、利用権管理装置 11aに送信する(図18; ステップ S31)。登録要求 Drscは、本機器 21cをユーザ情報 DB 113に登録するよう利用権管理装置 11aに要求するための情報である。ステップ S31をより具体的に説明すると、まず、登録要求生成部 220は、機器識別子格納部 211から機器識別子 I dvcを取り出し、さらに、グループ識別子格納部 221からグループ識別子 I qpを取り出した後、取り出したグループ識別子 I qpおよび機器識別子 I dvcの組み合わせに、予め保持する登録要求識別子 I rsを付加して、登録要求 Drsc(図19(a)参照)を生成する。ここで、登録要求識別子 I rsは、利用権管理装置 11aが登録要求 Drscを特定するために使用される。登録要求生成部 220は、以上の登録要求 Drscを通信部 213に渡す。通信部 213は、受け取った登録要求 Drscを、伝送路 31を通じて、利用権管理装置 11aに送信する。

【0096】利用権管理装置11a（図16参照）において、通信部115は、伝送路31を通じて送信されてくる情報を受信し、それに含まれる登録要求識別子1rsから、今回の受信情報が登録要求Drscであることを認識する。この認識結果に従って、通信部115は、受信登録要求Drscを、ユーザ情報管理部124に渡す。ユーザ情報管理部124は、受信登録要求Drscからグループ識別子1qpを取り出した後、ユーザ情報DB113にアクセスして、取り出したグループ識別子1qpを含む契約者レコードRcs（図7（a）参照）を検索する（ステップS32）。さらに、ユーザ情報管理部124は、検索した契約者レコードRcsから機器識別子数Ndvcを取り出す（ステップS33）。

【0097】次に、ユーザ情報管理部124は、取り出した機器識別子数Ndvcが予め定められた上限値Vul以上であるか否かを判断する（ステップS34）。ここで、上限値Vulは、ユーザβがユーザ情報DB113に登録可能な機器数の上限値である。ユーザ情報管理部124は、ステップS34で、機器識別子数Ndvcが上限値Vul以上でないと判断した場合には、受信登録要求Drscから機器識別子1dvcを取り出し、取り出したものを対象となる契約者レコードRcsに追加する（ステップS35）。さらに、ユーザ情報管理部124は、機器識別子数Ndvcを1だけインクリメントする（ステップS36）。その結果、契約者レコードRcsは、図7（a）に示すものから、図20に示すようなものに更新される。その後、ユーザ情報管理部124は、契約者レコードRcsを正しく更新した旨を登録完了生成部125に通知し、さらに、受信登録要求Drsc内の機器識別子1dvcを登録完了生成部125に渡す。

【0098】登録完了生成部125は、ユーザ情報管理部124から契約者レコードDrscの更新が完了したことが通知されると、図19（b）に示す登録完了通知Dscを生成し、機器21cに送信する（ステップS37）。登録完了通知Dscは、本機器21cをユーザ情報DB113に正しく登録したことを機器21cに通知するための情報である。ステップS37をより具体的に説明すると、まず、登録完了生成部125は、ユーザ情報管理部124から受け取った機器識別子1dvcに、予め保持する登録完了識別子1scを付加して、登録完了通知Dsc（図19（b）参照）を生成する。ここで、登録完了識別子1scは、機器21cが登録完了通知Dscを特定するために使用される。登録完了生成部125は、以上の登録完了通知Dscを通信部115に渡す。通信部115は、受け取った登録完了通知Dscを、伝送路31を通じて、機器21cに送信する。

【0099】機器21c（図17参照）において、通信部213は、伝送路31を通じて送信されてくる情報を受信し、それに含まれる登録完了識別子1scから、今回の受信情報が登録完了通知Dscであることを認識す

る。この認識結果に従って、通信部213は、受信登録完了通知Dscを、設定要求生成部212に渡す。設定要求生成部212は、受信情報に設定されている登録完了識別子1scから、今回登録完了通知Dscを受信したことを認識する（ステップS38）。この認識結果に従って、設定要求生成部212は図8のステップS11を実行可能な状態になったと判断し、以降は第1の実施形態で説明した機器21aまたは機器21bと同様に、利用権管理装置11aとデータ通信を行う。

【0100】以上のように本変型例によれば、利用権管理装置11aおよび機器21cのデータ通信により、ユーザβが新しい入手した機器21cの機器識別子1dvcを、ユーザ情報DB113に登録することが可能になるので、より使い勝手の良いライセンス情報管理システムSa1を提供できるようになる。

【0101】なお、ステップS34において、機器識別子数Ndvcが上限値Vul以上であると判断された場合、ユーザ情報管理部124は、ステップS35～S36のような処理を行わずに、契約者レコードRcsの更新を拒否する旨を登録完了生成部125に通知し、さらに、受信登録要求Drsc内の機器識別子1dvcを登録完了生成部125に渡す。登録完了生成部125は、契約者レコードDrscの更新拒否が通知されると、図19（c）に示す登録拒否通知Dsrcを生成し、通信部213および伝送路31を通じて、機器21cに送信する（ステップS39）。登録拒否通知Dsrcは、本機器21cをユーザ情報DB113に登録できないことを機器21cに通知するための情報であり、ユーザ情報管理部124から受け取った機器識別子1dvcと、予め保持する登録拒否識別子1srを含む。機器21c（図17参照）において、設定要求生成部212は、通信部213を通じて、登録拒否通知Dsrcを受け取り（ステップS310）、その通知に従って、設定要求生成部212は、図8のステップS11を実行可能な状態ではないと判断し、処理を終了する。

【0102】また、ステップS32において、ユーザ情報管理部124は、取り出したグループ識別子1qpを含む契約者レコードRcs（図7（a）参照）を見つけない場合には、ステップS39と同様の処理を行って、機器識別子1dvcのユーザ情報DB113への登録を拒否することが好ましい。

【0103】なお、以上の第1の変型例では、機器21cおよび利用権管理装置11aがデータ通信を行うことにより、機器識別子1dvcがユーザ情報DB113に登録されていた。しかし、これに限らず、以下の第2～第4の変型例のように、機器21cと、他の機器21aまたは機器21bとが協働して、機器識別子1dvcがユーザ情報DB113に登録されるようにしても良い。

【0104】「第2の変型例」次に、第2の変型例に係る利用権管理装置11bを収容したライセンス情報管理

システム S_{a2}の全体構成について説明する。ライセンス情報管理システム S_{a2}は、図 1 のライセンス情報管理システム S_aと比較すると、図 15 に示すように、利用権管理装置 11 に代えて利用権管理装置 11b を備えている点と、機器 21c をさらに備えている点で相違する。それ以外に両ライセンス情報管理システム S_a および S_{a2}に相違点はないので、図 15 において、図 1 の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【0105】利用権管理装置 11b は、上述の事業者 α 側に設置され、図 2 の利用権管理装置 11 と比較すると、図 21 に示すように、ユーザ情報管理部 126 と、登録完了生成部 127 とをさらに備える点で相違する。それ以外に両利用権管理装置 11 および 11b の間に相違点はない。それ故、図 21 において、図 2 の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【0106】機器 21a または機器 21b は、第 1 の実施形態で説明したように、ユーザ β により所有され、さらに、それぞれの機器識別子 1dva および 1dvb は、利用権管理装置 11b のユーザ情報 DB 113 に登録済みである（図 7（a）参照）。また、機器 21a または 21b は、機器 21c の機器識別子 1dvc の登録のために、図 4 と比較すると、図 22 に示すように、機器識別子入力部 222 と、仮登録要求生成部 223 と、仮登録完了出力部 224 とをさらに備える点で相違する。それ以外に、本変型例に係る機器 21a および 21b と、第 1 の実施形態に係るものとの間に相違点はない。それ故、図 22 において、図 4 の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【0107】機器 21c は、上述のユーザ β により所有されるが、現時点では、利用権管理装置 11b のユーザ情報 DB 113 に未登録の機器であって、図 4 の機器 21a または 21b と比較すると、図 23 に示すように、機器識別子入力部 225 および本登録要求生成部 226 をさらに備える点で相違する。それ以外に、両機器 21a および 21b と、機器 21c との間には相違点はない。それ故、図 23 において、図 4 の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【0108】次に、図 24 および図 25 を参照して、以上のような構成のライセンス情報管理システム S_{a2}において、機器 21c の機器識別子 1dvc をユーザ情報 DB 113 に登録するまでの機器 21a、機器 21c および利用権管理装置 11b の動作について説明する。ユーザ β は、機器 21a を操作して、機器識別子 1dvc をユーザ情報 DB 113 に仮登録する旨を指定する。この指定に関連して、機器 21a の機器識別子入力部 222 は、ユーザ β が機器 21a を操作することにより入力された機器 21c の機器識別子 1dvc を、仮登録要求生成部 2

23 に通知する（図 24：ステップ S41）。ここで、以下の説明では、機器 21c の機器識別子 1dvc を登録対象識別子 1dvc と称する。仮登録要求生成部 223 は、上述の通知に回答して、図 26（a）に示す仮登録要求 Dprsc を生成し、利用権管理装置 11b に送信する（ステップ S42）。仮登録要求 Dprsc は、登録対象識別子 1dvc をユーザ情報 DB 113 に仮登録するよう利用権管理装置 11b に要求するための情報である。ステップ S42 を具体的に説明すると、まず、仮登録要求生成部 223 は、機器識別子格納部 211 から機器識別子 1dva を取り出した後、取り出した機器識別子 1dva を登録済識別子 1dva として扱う。そして、仮登録要求生成部 223 は、登録済識別子 1dva および登録対象識別子 1dvc の組み合わせに、予め保持する仮登録要求識別子 1prs を付加して、仮登録要求 Dprsc（図 26（a）参照）を生成する。ここで、仮登録要求識別子 1prs は、利用権管理装置 11b が仮登録要求 Dprsc を特定するために使用される。仮登録要求生成部 223 は、以上の仮登録要求 Dprsc を通信部 213 に渡す。通信部 213 は、受け取った仮登録要求 Dprsc を、伝送路 31 を通じて、利用権管理装置 11b に送信する。

【0109】利用権管理装置 11b（図 21 参照）において、通信部 115 は、伝送路 31 からの受信情報に仮登録要求識別子 1prs が含まれていることから、仮登録要求 Dprsc を今回受信したことを認識する。この認識結果に従って、通信部 115 は、受信仮登録要求 Dprsc を、ユーザ情報管理部 126 に渡す。ユーザ情報管理部 126 は、受信仮登録要求 Dprsc から登録済識別子 1dva を取り出した後、ユーザ情報 DB 113 にアクセスして、取り出した登録済識別子 1dva を含む契約者レコード Rcs（図 7（a）参照）を検索する（ステップ S43）。その後、ユーザ情報管理部 126 は、図 18 のステップ S33 および S34 と同様の処理を行って（ステップ S44、S45）、ステップ S45 において、機器識別子数 Ndv が上限値 V_{ul} 未満でないと判断した場合に、図 18 のステップ S39 と同様の処理を行う（ステップ S46）。この場合、機器 21a は、図 18 のステップ S310 と同様の処理を行う（ステップ S47）。

【0110】それに対して、ステップ S45 において、機器識別子数 Ndv が上限値 V_{ul} 未満であると判断した場合に、受信仮登録要求 Dprsc から登録対象識別子 1dvc を取り出した後、取り出したものと、それが仮登録された機器識別子 1dvc であることを示す仮登録フラグ Fps とを、対象となる契約者レコード Rcs に追加する（ステップ S48）。契約者レコード Rcs は、図 7（a）に示すものから、図 27（a）に示すようなものに更新される。その後、ユーザ情報管理部 126 は、登録対象識別子 1dvc の仮登録が完了した旨を登録完了生成部 127 に通知し、さらに、受信仮登録要求 Dprsc 内の登録済識別子 1dva を登録完了生成部 127 に渡す。

【0111】登録完了生成部127は、ユーザ情報管理部126から仮登録が完了したことが通知されると、図26(b)に示す仮登録完了通知Dpsccを生成し、機器21aに送信する(ステップS49)。仮登録完了通知Dpsccは、登録対象識別子1dvcをユーザ情報DB113に仮登録したことを機器21aに通知するための情報である。ステップS48をより具体的に説明すると、まず、登録完了生成部127は、ユーザ情報管理部126から受け取った登録済識別子1dvaに、予め保持する仮登録完了識別子1pscを付加して、仮登録完了通知Dpscc(図26(b)参照)を生成する。ここで、仮登録完了識別子1pscは、機器21aが仮登録完了通知Dpsccを特定するために使用される。以上の仮登録完了通知Dpsccは、登録完了生成部127から、通信部115および伝送路31を通じて、機器21aに送信される。

【0112】機器21a(図22参照)において、通信部213は、伝送路31からの受信情報に含まれる仮登録完了識別子1pscおよび登録済識別子1dvaから、今回の受信情報が自分宛の仮登録完了通知Dpsccであることを認識する。この認識結果に従って、通信部213は、受信仮登録完了通知Dpsccを、仮登録完了出力部224に渡す。仮登録完了出力部224は、受信仮登録完了Dpsccに回答して、機器識別子1dvcの仮登録が完了したことを、画像または音声で出力し(ステップS410)、そのことをユーザβに伝える。これによって、機器21a側の処理が終了する。

【0113】仮登録完了を認識すると、ユーザβは、機器21cを操作して、機器識別子1dvcをユーザ情報DB113に本登録する旨を指定する。この指定に関連して、機器21cの機器識別子入力部225は、ユーザβが機器21cを操作することにより入力された機器21aの機器識別子(登録済識別子)1dvaを、本登録要求生成部226に通知する(図25;ステップS51)。この通知に回答して、本登録要求生成部226は、図28(a)に示す本登録要求Dcrscを生成し、利用権管理装置11bに送信する(ステップS52)。本登録要求Dcrscは、機器識別子1dvcをユーザ情報DB113に本登録するよう利用権管理装置11bに要求するための情報である。ステップS52を具体的に説明すると、まず、本登録要求生成部226は、機器識別子格納部211から機器識別子(つまり、登録対象識別子)1dvcを取り出した後、取り出した登録対象識別子1dvcと、通知された登録済識別子1dvaとの組み合わせに、予め保持する本登録要求識別子1crsを付加して、本登録要求Dcrsc(図28(a)参照)を生成する。ここで、本登録要求識別子1crsは、利用権管理装置11bが本登録要求Dcrscを特定するために使用される。本登録要求生成部226は、以上の本登録要求Dcrscを、通信部213および伝送路31を通じて、利用権管理装置11bに送信する。

【0114】利用権管理装置11b(図21参照)において、通信部115は、伝送路31からの受信情報に含まれる本登録要求識別子1crsから、今回の受信情報が本登録要求Dcrscであることを認識する。この認識結果に従って、受信本登録要求Dcrscはユーザ情報管理部126に渡され、ユーザ情報管理部126は、受信本登録要求Dcrscから、機器識別子1dvaおよび1dvcの双方を取り出した後、ユーザ情報DB113にアクセスして、取り出した両機器識別子1dvaおよび1dvcを含む契約者レコードRcs(図27(a)参照)を検索する(ステップS53)。その後、ユーザ情報管理部126は、検索した契約者レコードRcsから、仮登録フラグFpsを削除し(ステップS54)、さらに、それに含まれる機器識別子数Ndvcを1だけインクリメントする(ステップS55)。これによって、機器識別子1dvcの本登録が完了し、その結果、契約者レコードRcsは、図27(a)に示すものから、同図(b)に示すようなものに更新される。その後、ユーザ情報管理部126は、登録対象識別子1dvcの本登録が完了した旨を登録完了生成部127に通知し、さらに、受信本登録要求Dcrsc内の登録対象識別子1dvcを登録完了生成部127に渡す。

【0115】登録完了生成部127は、ユーザ情報管理部126から本登録が完了したことが通知されると、図28(b)に示す本登録完了通知Dcscを生成し、機器21cに送信する(ステップS56)。本登録完了通知Dcscは、ユーザ情報DB113に機器識別子1dvcの本登録が完了したことを機器21cに通知するための情報である。ステップS56をより具体的に説明すると、まず、登録完了生成部127は、ユーザ情報管理部126から受け取った登録対象識別子1dvcを登録済識別子1dvcとして扱い、これに、予め保持する本登録完了識別子1cscを付加して、本登録完了通知Dcsc(図28(b)参照)を生成する。ここで、本登録完了識別子1cscは、機器21cが本登録完了通知Dcscを特定するために使用される。以上の本登録完了通知Dcscは、通信部213および伝送路31を通じて、機器21cに送信される。

【0116】機器21c(図23参照)において、通信部213は、伝送路31を通じて送信されてくる情報を受信し、それに含まれる本登録完了識別子1cscおよび登録対象識別子1dvcから、今回の受信情報が自分宛の本登録完了通知Dcscであることを認識する。この認識結果に従って、通信部213は、受信本登録完了通知Dcscを、設定要求生成部212に渡す。設定要求生成部212は、受信情報に設定されている本登録完了識別子1cscから、今回本登録完了通知Dcscを受信したことを認識する(ステップS57)。この認識結果に従って、設定要求生成部212は図8のステップS11を実行可能な状態になったと判断し、以降は第1の実施形態で説明した機器21aまたは機器21bと同様に、利用

権管理装置 11b とデータ通信を行う。

【0117】前述の第1の変型例に係る機器識別子 1dvc の追加登録では、利用権管理装置 11a は、機器 21c が本当にユーザβにより所有されているか否かを判断できないまま、機器識別子 1dvc を、ユーザβの契約者レコード Rcs に登録していた。しかしながら、本変型例では、仮登録の時に機器 21a が送信する仮登録要求 Dprsc に、登録済識別子 1dva と、登録対象識別子 1dvc とが設定され、本登録の時に機器 21c が送信する本登録要求 Dcrsc に、登録済識別子 1dva と、登録対象識別子 1dvc とが設定されることにより、機器 21a および 21c の間に関連性があることを証明することが可能となる。これによって、利用権管理装置 11b は、機器 21c が機器 21a のユーザβにより所有されていると判断できる。このように、本変型例では、ユーザβの所有物でない機器 21c がユーザβの契約者レコード Rcs に登録されにくい、機器識別子の追加登録を行えるライセンス情報管理システム Sa2 を提供できるようになる。

【0118】なお、以上の変型例では、機器 21c の機器識別子 1dvc の追加登録のために、機器 21a が動作する例について説明した。しかし、これに限らず、機器 21b も機器 21a と同様に動作することで、機器識別子 1dvc の追加登録に関与できるようになる。

【0119】「第3の変型例」次に、第3の変型例に係る利用権管理装置 11c を收容したライセンス情報管理システム Sa3 の全体構成について説明する。ライセンス情報管理システム Sa3 は、図1のライセンス情報管理システム Sa と比較すると、図15に示すように、利用権管理装置 11 に代えて利用権管理装置 11c を備えている点と、機器 21c をさらに備えている点で相違する。それ以外に両ライセンス情報管理システム Sa および Sa3 に相違点はないので、図15において、図1の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【0120】利用権管理装置 11c は、上述の事業者α側に設置され、図2の利用権管理装置 11 と比較すると、図29に示すように、ユーザ情報管理部 128 と、パスワード通知生成部 129 と、登録完了生成部 130 とをさらに備える点で相違する。それ以外に両利用権管理装置 11 および 11c の間に相違点はない。それ故、図29において、図2の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【0121】機器 21a または機器 21b は、第1の実施形態で説明したように、ユーザβにより所有され、さらに、それぞれの機器識別子 1dva および 1dvb は、利用権管理装置 11c のユーザ情報 DB 113 に登録済みである(図7(a)参照)。また、機器 21a または 21b は、機器 21c の機器識別子 1dvc の登録のために、図4と比較すると、図30に示すように、パスワード入力部 227 と、登録要求生成部 228 と、登録完了

出力部 229 とをさらに備える点で相違する。それ以外に、本変型例に係る機器 21a および 21b と、第1の実施形態に係るものとの間に相違点はない。それ故、図30において、図4の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【0122】機器 21c は、上述のユーザβにより所有されるが、現時点では、利用権管理装置 11c のユーザ情報 DB 113 に未登録の機器であって、図4の機器 21a または 21b と比較すると、図31に示すように、機器識別子入力部 230、パスワード要求生成部 231 およびパスワード通知部 232 をさらに備える点で相違する。それ以外に、両機器 21a および 21b と、機器 21c との間には相違点はない。それ故、図31において、図4の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【0123】次に、図32および図33を参照して、以上のような構成のライセンス情報管理システム Sa3 において、機器 21c の機器識別子 1dvc をユーザ情報 DB 113 に登録するまでの機器 21a、機器 21c および利用権管理装置 11c の動作について説明する。ユーザβは、機器 21c を操作して、機器識別子 1dvc をユーザ情報 DB 113 に仮登録する旨を指定する。この指定に関連して、機器 21c の機器識別子入力部 230 は、ユーザβが機器 21c を操作することにより入力された機器 21a の機器識別子(以下、登録済識別子と称する) 1dva を、パスワード要求生成部 231 に通知する(図32; ステップ S61)。パスワード要求生成部 231 は、上述の通知に応答して、図34(a)に示すパスワード要求 Drps を生成し、利用権管理装置 11c に送信する(ステップ S62)。パスワード要求 Drps は、登録対象識別子 1dvc をユーザ情報 DB 113 に登録するために必要となるパスワード Wpss の発行を利用権管理装置 11c に要求するための情報である。ステップ S62 を具体的に説明すると、まず、パスワード要求生成部 231 は、機器識別子格納部 211 から登録対象識別子 1dvc を取り出した後、取り出した登録対象識別子 1dvc と、通知された登録済識別子 1dva とで構成される組みに、予め保持するパスワード要求識別子 1rps を付加して、パスワード要求 Drps (図34(a)参照)を生成する。ここで、パスワード要求識別子 1rps は、利用権管理装置 11c がパスワード要求 Drps を特定するために使用される。パスワード要求生成部 231 は、以上のパスワード要求 Drps を、通信部 213 および伝送路 31 を通じて、利用権管理装置 11c の通信部 115 に送信する。

【0124】利用権管理装置 11c (図29参照)において、通信部 115 は、受信情報内のパスワード要求識別子 1rps から、パスワード要求 Drps を今回受信したことを認識する。この認識結果に従って、通信部 115 は、受信パスワード要求 Drps を、ユーザ情報管理部 1

28に渡す。ユーザ情報管理部128は、受信パスワード要求Dppsから登録済識別子1dvaを取り出した後、ユーザ情報DB113にアクセスして、取り出した登録済識別子1dvaを含む契約者レコードRcs(図7(a)参照)を検索する(ステップS63)。その後、ユーザ情報管理部128は、図18のステップS33およびS34と同様の処理を行って(ステップS64、S65)、ステップS65において、機器識別子数Ndが上限値Vul以上であると判断した場合には、図18のステップS39と同様の処理を行う(ステップS66)。この場合、機器21cは、図18のステップS310と同様の処理を行う(ステップS67)。

【0125】それに対して、ステップS65において、機器識別子数Ndが上限値Vul以上でないと判断した場合に、ユーザ情報管理部128は、ステップS68を行い、まず、上述のパスワードWpssを生成する。パスワードWpssは、典型的には、ユーザ情報管理部128が無作為に選んだ文字または記号の組み合わせであることが好ましい。さらに、ユーザ情報管理部128は、受信パスワード要求Dppsから登録対象識別子1dvcを取り出した後、取り出したものと、生成したパスワードWpssとを、ステップS63で検索した契約者レコードRcsに追加して、登録対象識別子1dvcの仮登録を行う(ステップS68)。これによって、契約者レコードRcsは、図7(a)に示すものから、図35(a)に示すようなものに更新される。その後、ユーザ情報管理部128は、登録対象識別子1dvcの仮登録が完了した旨をパスワード通知生成部129に通知し、さらに、受信パスワード要求Dpps内の登録対象識別子1dvcおよびステップS68で生成したパスワードWpssを、パスワード通知生成部129に渡す。

【0126】パスワード通知生成部129は、ユーザ情報管理部128から仮登録が完了したことが通知されると、図34(b)に示すパスワード通知Dppsを生成し、機器21cに送信する(ステップS69)。パスワード通知Dppsは、登録対象識別子1dvcの登録のために生成したパスワードWpssを機器21cに通知するための情報である。ステップS69をより具体的に説明すると、まず、パスワード通知生成部129は、ユーザ情報管理部126から受け取った登録対象識別子1dvcおよびパスワードWpssの組み合わせに、予め保持するパスワード通知識別子1pssを付加して、パスワード通知Dpps(図34(b)参照)を生成する。ここで、パスワード通知識別子1pssは、機器21cがパスワード通知Dppsを特定するために使用される。以上のパスワード通知Dppsは、パスワード通知生成部129から、通信部115および伝送路31を通じて、機器21cの通信部213に送信される。

【0127】機器21c(図31参照)において、通信部213は、受信信号内のパスワード通知識別子1pss

および登録対象識別子1dvcから、今回の受信情報が自分宛のパスワード通知Dppsであることを認識する。この認識結果に従って、通信部213は、受信パスワード通知Dppsを、パスワード通知部232に渡す。パスワード通知部232は、パスワード通知Dppsに含まれるパスワードWpssを画像出力または音声出力することで、それをユーザβに通知する(ステップS610)。これによって、機器21c側の処理が終了する。なお、ステップS610において、パスワード通知部232は、パスワードWpssの通知に加えて、登録対象識別子1dvcの仮登録が終了したことを画像または音声でユーザβに伝えても良い。

【0128】仮登録完了を認識すると、ユーザβは、機器21aを操作して、機器識別子1dvcをユーザ情報DB113に本登録する旨を指定する。この指定に関連して、機器21aのパスワード入力部227は、ユーザβが機器21aを操作することにより入力されたパスワードWpssを、登録要求生成部228に通知する(図33;ステップS71)。この通知に回答して、登録要求生成部228は、図36(a)に示す登録要求Drscを生成し、利用権管理装置11cに送信する(ステップS72)。登録要求Drscは、登録対象識別子1dvcをユーザ情報DB113に本登録するよう利用権管理装置11cに要求するための情報である。ステップS72を具体的に説明すると、まず、登録要求生成部228は、機器識別子格納部211から機器識別子(つまり、登録済識別子)1dvaを取り出した後、取り出したものと、通知されたパスワードWpssとの組みに、予め保持する登録要求識別子1rsを付加して、登録要求Drsc(図36(a)参照)を生成する。ここで、登録要求識別子1rsは、利用権管理装置11cが登録要求Drscを特定するために使用される。登録要求生成部228は、以上の登録要求Drscを、通信部213および伝送路31を通じて、利用権管理装置11cに送信する。

【0129】利用権管理装置11c(図29参照)において、通信部115は、受信情報に含まれる登録要求識別子1rsから、今回の受信情報が登録要求Drscであることを認識する。この認識結果に従って、受信登録要求Drscはユーザ情報管理部128に渡され、ユーザ情報管理部128は、受信登録要求Drscから、登録済識別子1dvaおよびパスワードWpssの双方を取り出した後、ユーザ情報DB113にアクセスして、取り出した登録済識別子1dvaおよびパスワードWpssを含む契約者レコードRcs(図35(a)参照)を検索する(ステップS73)。その後、ユーザ情報管理部128は、検索した契約者レコードRcsから、パスワードWpssを削除し(ステップS74)、さらに、それに含まれる機器識別子数Ndを1だけインクリメントする(ステップS75)。これによって、機器識別子1dvcの本登録が完了し、その結果、契約者レコードRcsは、図35(a)

に示すものから、同図(h)に示すようなものに更新される。その後、ユーザ情報管理部128は、登録対象識別子1dvcの本登録が完了した旨を登録完了生成部130に通知し、さらに、受信登録要求Dpsc内の登録済識別子1dvaを登録完了生成部130に渡す。

【0130】登録完了生成部130は、ユーザ情報管理部128から本登録が完了したことが通知されると、図36(b)に示す登録完了通知Dscを生成し、機器21aに送信する(ステップS76)。登録完了通知Dscは、ユーザ情報DB113に機器識別子1dvcの本登録が完了したことを機器21aに通知するための情報である。ステップS76をより具体的に説明すると、まず、登録完了生成部130は、ユーザ情報管理部128から受け取った登録済識別子1dvaに、予め保持する登録完了識別子1scを付加して、登録完了通知Dsc(図36(b)参照)を生成する。ここで、登録完了識別子1scは、機器21aが本登録完了通知Dscを特定するために使用される。以上の登録完了通知Dscは、通信部115および伝送路31を通じて、機器21aの通信部213に送信される。

【0131】機器21a(図30参照)において、通信部213は、受信情報に含まれる登録完了識別子1scおよび登録済識別子1dvaから、今回の受信情報が自分宛の登録完了通知Dscであることを認識する。この認識結果に従って、通信部213は、受信本登録完了通知Dscを、登録完了出力部229に渡す。登録完了出力部229は、受信情報内の登録完了識別子1scから、今回登録完了通知Dscを受信したことを認識し、登録対象識別子1dvcの本登録が完了したことを画像出力または音声出力して(ステップS77)、ユーザβにその旨を伝える。これによって、機器21cは、図8のステップS11を実行可能な状態になる。そして、機器21cは、必要に応じて、以降は第1の実施形態で説明した機器21aまたは機器21bと同様の処理を行って、コンテンツデータDcntを利用する。

【0132】上述の第3の変型例によれば、利用権管理装置11cのユーザ情報DB113に登録済みの機器21aが、未登録の機器21cの機器識別子1dvcの登録に関与することで、第2の変型例と同様に、ユーザβの所有物でない機器21cがユーザβの契約者レコードRcsに登録されにくい、機器識別子の追加登録を行えるライセンス情報管理システムSa3を提供できるようになる。

【0133】なお、以上の変型例では、機器21cの機器識別子1dvcの追加登録のために、機器21aが動作する例について説明した。しかし、これに限らず、機器21bも機器21aと同様に動作することで、機器識別子1dvcの追加登録に関与できるようになる。

【0134】「第4の変型例」次に、第4の変型例に係る利用権管理装置11dを収容したライセンス情報管理システムSa4の全体構成について説明する。ライセンス

情報管理システムSa4は、図1のライセンス情報管理システムSaと比較すると、図15に示すように、利用権管理装置11に代えて利用権管理装置11dを備えている点と、機器21cをさらに備えている点と、機器21aおよび21cが通信ケーブル32を介して通信可能に接続される点とで相違する。それ以外に両ライセンス情報管理システムSaおよびSa4に相違点はないので、図15において、図1の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【0135】利用権管理装置11dは、上述の事業者α側に設置され、図2の利用権管理装置11と比較すると、図37に示すように、ユーザ情報管理部131と、登録完了生成部132とをさらに備える点で相違する。それ以外に両利用権管理装置11および11dの間に相違点はない。それ故、図37において、図2の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【0136】機器21aまたは21bは、第1の実施形態で説明したように、ユーザβにより所有され、さらに、それぞれの機器識別子1dvaおよび1dvbは、利用権管理装置11dのユーザ情報DB113に登録済みである(図7(a)参照)。また、機器21aまたは21bは、機器21cの機器識別子1dvcの登録のために、図4と比較すると、図38に示すように、通信部228と、登録要求生成部229と、登録完了通知部230とをさらに備える点で相違する。それ以外に、本変型例に係る機器21aおよび21bと、第1の実施形態に係るものとの間に相違点はない。それ故、図38において、図4の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【0137】機器21cは、上述のユーザβにより所有されるが、現時点では、自身に割り当てられた機器識別子1dvcが利用権管理装置11dのユーザ情報DB113に未登録であって、図4の機器21aまたは21bと比較すると、図39に示すように、登録要求生成部231と、通信部232とをさらに備える点で相違する。それ以外に、図4の両機器21aおよび21bと、機器21cとの間には相違点はない。それ故、図39において、図4の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【0138】次に、図40を参照して、以上のような構成のライセンス情報管理システムSa4において、機器21cの機器識別子1dvcをユーザ情報DB113に登録するまでの機器21a、機器21cおよび利用権管理装置11dの動作について説明する。ユーザβは、機器21cを操作して、機器識別子1dvcをユーザ情報DB113に登録する旨を指定する。この指定に回答して、機器21cの登録要求生成部231は、図41(a)に示す第1の登録要求Dpsc1を生成し、通信ケーブル32を通じて、機器21aに送信する(図40:ステップS8

1)。第1の登録要求Drsclは、登録対象識別子ldvcをユーザ情報DB113に登録することを、機器21cの代わりに機器21aに要求するための情報である。ステップS81を具体的に説明すると、まず、登録要求生成部231は、機器識別子格納部211から機器識別子(以下、登録対象識別子と称する)ldvcを取り出した後、取り出した登録対象識別子ldvcに、予め保持する第1の登録要求識別子lrs1を付加して、第1の登録要求Drscl(図41(a)参照)を生成する。ここで、第1の登録要求識別子lrs1は、機器21aが第1の登録要求Drsclを特定するために使用される。登録要求生成部231は、以上の第1の登録要求Drsclを、通信部232および通信ケーブル32を通じて、機器21aに送信する。

[0139]機器21a(図38参照)において、通信部228は、受信情報内の第1の登録要求識別子lrs1から、第1の登録要求Drsclを今回受信したことを認識する(ステップS82)。この認識結果に従って、通信部228は、受信した第1の登録要求Drsclを、登録要求生成部229に渡す。それに従って、登録要求生成部229は、図41(b)に示す第2の登録要求Drsclを生成し、伝送路31を通じて、利用権管理装置11dに送信する(ステップS83)。第2の登録要求Drsclは、登録対象識別子ldvcをユーザ情報DB113に登録することを、利用権管理装置11dに要求するための情報である。ステップS83を具体的に説明すると、まず、登録要求生成部229は、機器識別子格納部211から機器識別子(以下、登録済識別子と称する)ldvaを取り出した後、取り出した登録済識別子ldvaを、今回受信した第1の登録要求Drsclに付加して、第2の登録要求Drscl(図41(b)参照)を生成する。ここで、第2の登録要求Drsclにおいて、第1の登録要求識別子lrs1は、利用権管理装置11dが第2の登録要求Drsclを特定するために使用される。登録要求生成部229は、以上の第2の登録要求Drsclを、通信部213および伝送路31を通じて、利用権管理装置11d(図37参照)に送信する。

[0140]利用権管理装置11dにおいて、通信部115は、伝送路31からの受信情報内の第1の登録要求識別子lrs1から、第2の登録要求Drsclを今回受信したことを認識する。その認識結果に従って、通信部115は、受信した第2の登録要求Drsclをユーザ情報管理部131に渡す。それに従って、ユーザ情報管理部131は、受信した第2の登録要求Drsclから登録済識別子ldvaを取り出し、ユーザ情報DB113にアクセスした後、図32のステップS63～S65と同様の処理を行う(ステップS84～S86)。ユーザ情報管理部131は、ステップS86において、機器識別子数Ndvが上限値Vul以上でないと判断した場合には、受信した第2の登録要求Drsclから登録対象識別子ldvcを取り

出した後、取り出したものを、ステップS84で検索した契約者レコードRcsに追加して、登録対象識別子ldvcの登録を行う(ステップS87)。これによって、契約者レコードRcsは、図7(a)に示すものから、図35(a)に示すようなものに更新される。その後、ユーザ情報管理部131は、登録対象識別子ldvcの登録が完了した旨を登録完了生成部132に通知し、さらに、受信した第2の登録要求Drscl内の登録済識別子ldvaを、登録完了生成部132に渡す。

[0141]登録完了生成部132は、ユーザ情報管理部131から登録完了が通知されると、図41(c)に示す登録完了通知Dscclを生成し、機器21aに送信する(ステップS88)。登録完了通知Dscclは、登録対象識別子ldvcのユーザ情報DB113への登録が完了したことを機器21aに通知するための情報である。ステップS88をより具体的に説明すると、まず、登録完了生成部132は、ユーザ情報管理部131から受け取った登録済識別子ldvaに、予め保持する登録完了識別子lscを付加して、登録完了通知Dsccl(図41(c)参照)を生成する。ここで、登録完了識別子lscは、機器21aが登録完了通知Dscclを特定するために使用される。以上の登録完了通知Dscclは、登録完了生成部132から、通信部115および伝送路31を通じて、機器21aの通信部213に送信される。

[0142]機器21a(図38参照)において、通信部213は、受信信号内の登録完了識別子lscおよび登録済識別子ldvaから、今回の受信情報が自分宛の登録完了通知Dscclであることを認識する。この認識結果に従って、通信部213は、受信登録完了通知Dscclを、登録完了通知部230に渡す。それに従って、登録完了通知部230は、登録対象識別子ldvcの登録が完了したことを画像出力または音声出力することで、それをユーザβに通知する(ステップS610)。これによって、ユーザβは、機器21cの機器識別子ldvcが登録されたことを認識し、機器21cは、図8のステップS11を実行可能な状態になる。そして、機器21cは、必要に応じて、以降は第1の実施形態で説明した機器21aまたは機器21bと同様の処理を行って、コンテンツデータDcntを利用する。

[0143]また、ステップS86において、機器識別子数Ndvが上限値Vul以上であると判断された場合、従前の実施形態と同様に、利用権管理装置11dから機器21aに、登録拒否通知Drsclが送信される(ステップS810、S811)。

[0144]上述の第4の変型例によれば、利用権管理装置11dのユーザ情報DB113に登録済みの機器21aが、未登録の機器21cの機器識別子ldvcの登録に関与することで、第2の変型例と同様に、ユーザβの所有物でない機器21がユーザβの契約者レコードRcsに登録されにくい、機器識別子の追加登録を行えるライ

センス情報管理システムS_{a4}を提供できるようになる。さらに、本変型例では、図32および図33の組み合わせと、図40とを比較すれば分かるように、機器21aおよび21cをケーブル32で通信可能に接続することで、機器識別子1dvcの登録までに必要な処理を減らすことができる。

【0145】なお、以上の変型例では、機器21cの機器識別子1dvcの追加登録のために、機器21aが動作する例について説明した。しかし、これに限らず、機器21bも機器21aと同様に動作することで、機器識別子1dvcの追加登録に関与できるようになる。

【0146】また、以上の変型例では、機器21aおよび機器21cを通信可能に接続するために通信ケーブル32を用いたが、これに限らず、機器21aおよび21cは無線通信を行っても良い。他にも、機器21aおよび21cは伝送路31を介して通信を行っても良い。

【0147】また、以上の変型例では、登録完了通知D_{scc}は、利用権管理装置11dから機器21aに送信されていた。しかし、これに限らず、利用権管理装置11dから機器21cに送信されても良い。また、機器21aに送信された登録完了通知D_{scc}は機器21cに転送されても良い。この場合、登録完了したことは、機器21cから音声または画像によりユーザβに通知される。

【0148】また、以上の第2～第4の変型例では、単一の機器21cの機器識別子1dvcをユーザ情報DB113に追加登録するための処理について説明したが、2台以上の機器21の機器識別子1dvを追加する場合にも、第2～第4の変型例を容易に応用することができる。

【0149】また、以上の第2～第4の変型例では、機器識別子1dvcの追加登録に関与できるのは、機器21aでも、機器21bでも良いと説明した。しかし、これに限らず、機器21aおよび21bのいずれか一方に、機器識別子1dvの追加登録に関与できる権限を与え、権限を持つ機器21のみが機器識別子1dvの追加登録に関与できるようにしても良い。

【0150】また、以上の第1～第4の変型例において、ユーザ情報DB113には、図7(a)に示す情報の他に、ユーザβに関連するユーザ情報をさらに登録しておき、機器21aまたは21cは、利用権管理装置11a～11dにアクセスする際に、ユーザβにより入力されたユーザ情報を送信する。利用権管理装置11a～11dは、受信ユーザ情報を、予め格納されているユーザ情報と照合することで、機器21cが機器21aと同じユーザβにより所有されているか否かを判断するようにしても良い。

【0151】また、第1の実施形態では、ユーザ情報DB113に契約時に登録された機器21aおよび21bが同一の利用権情報D_{rqt}を共有する例について説明した。しかし、ユーザβは、ユーザ情報DB113または

利用権DB114から、既に登録されている機器21bの機器識別子1dvbを削除したい場合がある。以下に説明する利用権管理装置11eは、上述の利用権管理装置11の第5の変型例であって、上述のニーズに対応するために提供される。

【0152】「第5の変型例」図42は、利用権管理装置11eを収容したライセンス情報管理システムS_{a5}の全体構成を示すブロック図である。ライセンス情報管理システムS_{a5}は、図1のライセンス情報管理システムS_aと比較すると、利用権管理装置11が利用権管理装置11eに代わる点でのみ相違する。それ以外に両ライセンス情報管理システムS_aおよびS_{a5}に相違点はない。それ故、図42において、図1の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【0153】利用権管理装置11eは、上述の事業者α側に設置され、図2の利用権管理装置11と比較すると、図43に示すように、機器識別子削除部133および削除完了作成部134をさらに備える点で相違する。それ以外に両利用権管理装置11および11eの間に相違点はない。それ故、図43において、図2の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【0154】機器21aまたは21bは、第1の実施形態で説明したように、ユーザβにより所有され、さらに、それぞれの機器識別子1dvaおよび1dvbは、利用権管理装置11eのユーザ情報DB113に登録済みである(図7(a)参照)。さらに、機器21aおよび21bは、利用権管理装置11eの利用権DB114に登録されている利用権レコードR_{rqt}を共有している(図7(b)参照)。また、機器21bは、機器識別子1dvbの削除のために、図4と比較すると、図44に示すように、削除要求生成部233と、削除完了通知部234とをさらに備える点で相違する。それ以外に、本変型例に係る機器21bと、第1の実施形態に係るものとの間に相違点はない。それ故、図44において、図4の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【0155】次に、図45を参照して、以上のような構成のライセンス情報管理システムS_{a5}において、機器21bの機器識別子1dvbをユーザ情報DB113および利用権DB114から削除するまでの機器21bおよび利用権管理装置11eの動作について説明する。ユーザβは、機器21bを操作して、機器識別子1dvbをユーザ情報DB113および利用権DB114から削除する旨を指定する。この指定に回答して、機器21bにおいて、削除要求生成部233は、図46(a)に示す削除要求D_{nwb}を生成し、利用権管理装置11eに送信する(図45;ステップS91)。削除要求D_{nwb}は、本機器21bをユーザ情報DB113および利用権DB114から削除するよう利用権管理装置11eに要求するた

めの情報である。ステップ S91 をより具体的に説明すると、まず、削除要求生成部 233 は、機器識別子格納部 211 から機器識別子 1 dvb を取り出した後、取り出したものを削除対象識別子 1 dvb として、予め保持する削除要求識別子 1 nv を付加して、削除要求 D nvb (図 46 (a) 参照) を生成する。ここで、削除要求識別子 1 nv は、利用権管理装置 11e が削除要求 D nvb を特定するために使用される。以上の削除要求 D nvb は、削除要求生成部 233 から、通信部 213 および伝送路 31 を通じて、利用権管理装置 11e に送信される。

【0156】利用権管理装置 11e (図 43 参照) において、通信部 115 は、伝送路 31 からの受信情報に含まれる削除要求識別子 1 nv から、今回の受信情報が削除要求 D nvb であることを認識する。この認識結果に従って、通信部 115 は、受信削除要求 D nvb を、機器識別子削除部 133 に渡す。機器識別子削除部 133 は、受信削除要求 D nvb から削除対象識別子 1 dvb を取り出した後、ユーザ情報 DB 113 内の契約者レコード R cs (図 7 (a) 参照) から、取り出した削除対象識別子 1 dvb を検索して削除する (ステップ S92)。さらに、機器識別子削除部 133 は、ステップ S92 で検索した契約者レコード R cs に含まれる機器識別子数 N dv を 1 だけデクリメントする (ステップ S93)。その結果、契約者レコード R cs は、図 7 (a) に示すものから、図 47 (a) に示すようなものに更新される。

【0157】さらに、機器識別子削除部 133 は、利用権 DB 114 内の利用権レコード R rqt から、受信削除要求 1 nvb から取り出した削除対象識別子 1 dvb を検索して削除する (ステップ S94)。その結果、利用権レコード R rqt は、図 7 (b) に示すものから、図 47 (b) に示すようなものに更新される。その後、機器識別子削除部 133 は、契約者レコード R cs および利用権レコード R rqt を正しく更新した旨と、受信登録要求 D rsc 内の削除対象識別子 1 dvb とを削除完了生成部 134 に通知する。

【0158】削除完了生成部 134 は、削除対象識別子 1 dvb の削除が完了したことが通知されると、図 46 (b) に示す削除完了通知 D swb を生成し、機器 21b に送信する (ステップ S95)。削除完了通知 D swb は、削除対象識別子 1 dvb を削除したことを機器 21b に通知するための情報である。ステップ S95 をより具体的に説明すると、まず、削除完了生成部 134 は、受け取った削除対象識別子 1 dvb に、予め保持する削除完了識別子 1 sw を付加して、削除完了通知 D swb (図 46 (b) 参照) を生成する。ここで、削除完了識別子 1 sw は、機器 21b が削除完了通知 D swb を特定するために使用される。以上の削除完了通知 D swb は、通信部 115 および伝送路 31 を通じて、機器 21b に送信される。

【0159】機器 21b (図 43 参照) において、通信

部 213 は、伝送路 31 からの受信情報に含まれる削除完了識別子 1 sw から、今回の受信情報が削除完了通知 D swb であることを認識する。この認識結果に従って、通信部 213 は、受信削除完了通知 D swb を、削除完了通知部 234 に渡す。削除完了通知部 234 は、削除完了通知 D swb を受信し (ステップ S96)、その後、機器識別子 1 dvb が正常に削除されたことを、画像または音声で出力して、ユーザにその旨を通知する。

【0160】以上のように本変型例によれば、利用権管理装置 11e および機器 21b のデータ通信により、ユーザが不必要となった機器 21b の機器識別子 1 dvb を、ユーザ情報 DB 113 および利用権 DB 114 から削除することが可能になるので、より使い勝手の良いライセンス情報管理システム S a5 を提供できるようになる。

【0161】なお、以上の変型例では、機器 21b 自身が、機器識別子 1 dvb の削除要求 D nvb を生成して利用権管理装置 11e に送信するようにしたが、これに限らず、機器 21a が、機器 21b の代わりに、削除要求 D nvb を生成して、利用権管理装置 11e に送信するようにしても良い。さらに、機器 21a および 21b のいずれかに削除要求 D nvb を生成する権限を与え、権限が与えられた機器 21a または 21b のみが削除要求 D nvb を利用権管理装置 11e に送信可能にしても良い。

【0162】また、以上の変型例では、削除要求 D nvb には、1 個の削除対象識別子 1 dvb が設定されるように説明したが、これに限らず、複数の機器識別子 1 dv が設定されても良い。さらに、削除要求 D nvb が、第 1 の実施形態で説明したグループ識別子 1 qp を含んでいる場合には、利用権管理装置 11e は、ユーザ情報 DB 113 から、そのグループ識別子 1 qp を含む契約者レコード R cs を削除し、さらに、利用権 DB 114 から、そのグループ識別子 1 qp を含む利用権レコード R rqt の全てを削除するようにしても良い。

【0163】「第 2 の実施形態」図 48 は、本発明の第 2 の実施形態に係る利用権管理装置 41 を収容したライセンス情報管理システム S b の全体構成を示すブロック図である。図 48 において、ライセンス情報管理システム S b は、利用権管理装置 41 の他に、複数の機器 51 の一例として 2 つの機器 51a および 51b と、伝送路 61 とを備えている。利用権管理装置 41 は、コンテンツ配信に関わる事業者 α 側に設置される。また、機器 51a および 51b は、典型的には、事業者 α との契約に基づいてコンテンツ配信を受ける契約者 β より使用される。また、伝送路 61 は、有線または無線であり、利用権管理装置 41 と、機器 51a または機器 51b とをデータ通信可能に接続する。

【0164】次に、図 49 を参照して、図 48 の利用権管理装置 41 の詳細な構成について説明する。図 49 の利用権管理装置 41 は、図 2 の利用権管理装置 11 と比

較すると、利用権データベース114および利用権管理部117の代わりに、利用権データベース（以下、利用権DBと称す）411および利用権管理部412を備えている点で相違する。それ以外に、両利用権管理装置11および41の間に構成面での相違点はない。それ故、図49において、図2の利用権管理装置11の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略すると共に、本実施形態で説明が不要となる構成の図示を省略する。

【0165】次に、図50を参照して、図48の機器51aおよび51bの詳細な構成について説明する。図50の機器51aおよび51bは、図4の機器21aおよび21bと比較して、設定要求生成部212の代わりに、設定要求生成部511を備えている点で相違する。それ以外に、機器51aおよび51bと、機器21aおよび21bとの間に構成面での相違点はない。それ故、図50において、図4の機器21aまたは21bの構成に相当するものには同一の参照符号を付け、それぞれの説明を省略すると共に、本実施形態で説明が不要となる構成の図示を省略する。

【0166】次に、上記ライセンス情報管理システムSbにおいても、前述のライセンス情報管理システムSaの場合と同様に、契約者βは事業者αからコンテンツ配信を受けるために必要となる準備を行う。この準備作業において、図6(a)、図6(b)および図7(a)に示すコンテンツDB111、復号鍵DB112およびユーザ情報DB113とが構築される。これらの詳細については、第1の実施形態で既に詳述しているため、本実施形態ではそれぞれの説明を省略する。

【0167】また、以上の準備作業において、事業者αは、機器51aおよび51bに、それらを一意に特定するための機器識別子1dvaおよび1dvbを割り当てる場合がある。以上の機器識別子1dvaは、図50に示す機器51aの機器識別子格納部211に設定され、機器識別子1dvbは、機器51bの機器識別子格納部211に設定される。なお、機器識別子1dvaおよび1dvbは、工場出荷時にそれぞれの機器識別子格納部211に設定されていても良い。

【0168】以上の準備が終了すると、機器51aおよび51bの一方は、ユーザβの操作に従って、利用権管理装置41から、コンテンツデータDcntを取得することが可能となる。以下、図51のフローチャートを参照して、コンテンツデータDcntの取得時における機器51aおよび利用権管理装置41の間のデータ通信、およびそれに関連するそれぞれの動作について説明する。なお、コンテンツデータDcntの取得時における機器51bおよび利用権管理装置41の間のデータ通信、およびそれに関連するそれぞれの動作については、機器51aのものと同様であるため、それぞれの説明を省略する。ここで、図51は、図8と比較すると、ステップS10

1およびS103をさらに含む点と、ステップS13の代わりにステップS102を含む点とで相違する。それ以外に両フローチャートに相違点はないので、図51において、図8のステップに相当するものには同一のステップ番号を付け、それぞれの説明を省略する。

【0169】ユーザβは、機器51aを操作して、利用権管理装置41にアクセスし、コンテンツDB111内のコンテンツデータDcntから、今回取得したいもののコンテンツ識別子1cntを指定する。以降の説明において、今回指定されたコンテンツデータDcntを、取得対象コンテンツデータDcntと称する。さらに、ユーザβは、取得対象コンテンツデータDcntを利用する際の利用条件Ccnt（第1の実施形態参照）を指定する。

【0170】この指定に回答して、機器51aの設定要求生成部511は、今回指定されたものの中に共有対象識別子1dvが含まれているか否かを判断する（ステップS101）。ここで、共有対象識別子1dvとは、本ステップS101を実行する機器51以外の他の機器51の機器識別子1dvであって、共有対象となる利用権レコードRrctaに登録済の機器51の機器識別子1dvである。上述から明らかなように、今回指定されるものには、共有対象識別子1dvは含まれないので、設定要求生成部511は、図9(a)の同様の形式を有する第1の設定要求Drra（第1の実施形態参照）を生成し、伝送路61を通じて、利用権管理装置41に送信する（ステップS11）。本実施形態において、第1の設定要求Drraに含まれる設定要求識別子1rrは、利用権管理装置41が受信情報が第1の設定要求Drraおよび第2の設定要求Drr2bのいずれかであることを特定するために使用される。

【0171】利用権管理装置41（図49参照）において、ユーザ認証部116は、伝送路61からの第1の設定要求Drraの受信に回答して、認証処理を行い（ステップS12）、その後、受け取った第1の設定要求Drraを利用権管理部412に渡す。利用権管理部412は、ユーザ認証部116からの受信情報内の設定要求識別子1rrに基づいて、今回の受信情報が第1の設定要求Drraまたは第2の設定要求Drr2bのいずれかであることを認識する。この認識結果に従って、利用権管理部412は、利用権データベース（以下、利用権DBと称する）114への利用権登録処理を行う（ステップS102）。ステップS102において、より具体的には、利用権管理部412は、今回、第1の設定要求Drraを受信したか否かを判断する（ステップS1021）。ここで、ステップS1021では、受信情報が共有対象識別子1dvを含んでいる場合には、第1の設定要求Drraを受信したと、利用権管理部412は判断する。それに対して、共有対象識別子1dvを含んでいない場合には、後述する第2の設定要求Drr2bを受信したと、利用権管理部412は判断する。今回の場合、利用権管理部

412は、第1の設定要求Drraを受信したと判断することになるから、ステップS1022を行う。

【0172】ステップS1022において、利用権管理部412は、受信した第1の設定要求Drraから、機器識別子Idva、コンテンツ識別子Icntおよび利用条件Ccntを取り出す。さらに、利用権管理部412は、利用権DB411にアクセスして、取り出したものを利用権レコードRrqaとして登録する(ステップS1022)。ここで、第1の実施形態と同様に、利用条件Ccntは、利用権情報Drratとして使われる。以上のステップS1022により、利用権DB114は、図52

(a)に示すように、機器識別子Idvaおよび/または機器識別子Idvb、コンテンツ識別子Icntならびに利用権情報Drratを含む利用権レコードRrqaの集まりとなる。ところで、第1の実施形態では、図8のステップS132およびS133で説明したように、利用権管理部117は、機器21aの設定要求Drraの受信に回答して、ユーザ情報DB113から同一グループに属する全機器識別子IdvaおよびIdvbを取り出し、それらを全て利用権レコードRrqaに登録していた。それに対して、第2の実施形態では、利用権管理部412は、ステップS1022の時点では、第1の設定要求Drraの送信元となる機器識別子Idvaのみを利用権レコードRrqaに登録する。この点で、第1および第2の実施形態は顕著に相違する。

【0173】以上のステップS1022が終了すると、今回受け取った第1の設定要求Drraを、利用権管理部412はコンテンツ管理部118に渡す。以降、利用権管理装置41は、利用権管理装置11と同様に、ステップS14～S17を実行し、その後、機器51aは、機器21aと同様に、ステップS18～S19を実行する。その結果、機器51aは、利用権管理装置41から、図9(b)に示す形式を有する送信データDtmaを受信する。また、本ライセンス情報管理システムSbにおいても、機器51aは、暗号済コンテンツデータDecntを復号するために、ライセンス情報Dlca(第1の実施形態参照)を利用権管理装置41から受け取るが、この時の動作については第1の実施形態と同様であるため(図11、図12参照)、その説明を省略する。

【0174】また、機器51bが利用権管理装置41に利用権レコードRrqaの新規登録を要求する場合には、上述の機器51aと利用権管理装置41の間で行われたデータ通信と同様の動作が行われるので、その説明を省略する。

【0175】ユーザβは、機器51aを使って、機器51bのために生成された利用権情報Drratを使いたい場合がある。このような場合、ユーザβは、機器51aを操作して、コンテンツ識別子Icntを指定し、さらに、共有対象識別子Idvとしての機器識別子Idvbを指定する。ここで注意を要するのは、機器51aが、機器51

bが既に設定した利用権情報Drratを共有することから、ユーザβは、利用条件Ccntを特に指定する必要性が無い点である。以上の指定に回答して、機器51aの設定要求生成部511は、今回指定されたものの中に、共有対象識別子Idvが含まれているか否かを判断する(ステップS101)。上述から明らかなように、今回指定されるものには、共有対象識別子Idvとしての機器識別子Idvbが含まれるので、設定要求生成部511は、図53に示す第2の設定要求Drr2aを生成し、伝送路61を通じて、利用権管理装置41に送信する(ステップS103)。第2の設定要求Drr2aは、他の機器51bのために登録済の利用権情報Drratの共有設定を利用権管理装置41に要求するための情報でもあり、本実施形態ではさらに、取得対象コンテンツデータDcntの配信を利用権管理装置41に要求するための情報である。ステップS103をより具体的に説明すると、まず、設定要求生成部511は、機器識別子格納部211から機器識別子Idvaを受け取る。設定要求生成部511は、ユーザβが指定したコンテンツ識別子Icntおよび共有対象識別子Idvbに、取り出した機器識別子Idvaと、予め保持する設定要求識別子Irrとを付加して、第2の設定要求Drr2a(図53参照)を生成する。以上の第2の設定要求Drr2aは、設定要求生成部511から通信部213および伝送路61を通じて、利用権管理装置41に送信される。

【0176】利用権管理装置41(図49参照)において、ユーザ認証部116は、伝送路61からの第2の設定要求Drr2aの受信に回答して、認証処理を行い(ステップS12)、その後、受け取った第2の設定要求Drr2aを利用権管理部412に渡す。利用権管理部412は、ユーザ認証部116から第2の設定要求Drr2aを受信したことに回答して、利用権DB114への利用権登録処理を行う(ステップS102)。ステップS102において、利用権管理部412は、今回、第1の設定要求Drraを受信したか否かを判断する(ステップS1021)。ここで、第2の設定要求Drr2aには共有対象識別子Idvbが含まれるので、利用権管理部412は、第1の設定要求Drraを受信していないと判断することになるから、ステップS1023を行う。

【0177】ステップS1023において、利用権管理部412は、受信した第2の設定要求Drr2aから、共有対象識別子Idvbおよびコンテンツ識別子Icntを取り出す。その後、利用権管理部412は、利用権DB411にアクセスして、取り出した共有対象識別子Idvbおよびコンテンツ識別子Icntの双方を含む利用権レコードRrqaを検索する。さらに、利用権管理部412は、受信した第2の設定要求Drr2aから機器識別子Idvaを取り出し、検索した利用権レコードRrqaに追加登録する(ステップS1024)。以上のステップS1024により、利用権DB114において、利用権レコードR

51

rqtaは、図52(b)に示すように、機器識別子I dvaおよびI dvb、コンテンツ識別子I cntならびに利用権情報D rqtを含むものに更新される。これによって、コンテンツデータD cntの利用権情報D rqtは、機器51aおよび51bからなるサブグループにより共有されていることが示される。以上のステップS1025が終了すると、今回受け取った第2の設定要求D rr2aを、利用権管理部412はコンテンツ管理部118に渡す。以降、利用権管理装置41は、ステップS14~S17を実行し、その後、機器51bは、ステップS18~S19を実行する。また、本ライセンス情報管理システムSbにおいても、機器51aは、暗号済コンテンツデータDecntを復号するために、ライセンス情報D lcb(第1の実施形態参照)を利用権管理装置41から受け取る。この時、機器51aおよび利用権管理装置41では、第1の実施形態で機器21bおよび利用権管理装置11が行った処理と同様に、図11および図12に示す処理が行われる。

【0178】以上のように本実施形態によれば、利用権レコードR rqtには、複数の機器識別子I dvaおよびI dvbが記録される。これによって、利用権管理装置41は、互いに異なる機器51aおよび51bから発行要求D iraおよびD irbが送信されてきたとしても、利用権レコードR rqtを参照することで、同一の利用権情報D rqtから生成されたライセンス情報D lcaおよびD lcbをそれらに提供することができるようになる。以上の本実施形態によって、複数の機器が共通のデジタルライツを共有できる権利管理技術を提供することができる。

【0179】さらに、第1の実施形態では、ユーザβが所有する複数の機器21の1台が設定要求D rrを利用権管理装置11に送信すれば、利用権管理装置11は、そのユーザβが所有する全機器21の機器識別子I dvを権利レコードR rqtに一括的に登録していた。それに対して、本実施形態では、機器51が第2の設定要求D rr2を送信しない限り、利用権管理装置41は、その送信元の機器識別子I dvを権利レコードR rqtに登録しない。これによって、利用権情報D rqtの共有をより厳密に制御することが可能となる。

【0180】なお、以上の第2の実施形態に係るライセンス情報管理システムSbも、第1の実施形態に係るライセンス情報管理システムSaと同様に、前述した第2~第5の変型例のような処理を利用権管理装置41ならびに機器51aおよび51bに組み込むことで、機器識別子I dvaおよび/またはI dvbの追加または削除が可能になる。

【0181】「第3の実施形態」図54は、第3の実施形態に係るライセンス情報管理システムScの全体構成を示すブロック図である。図54において、ライセンス情報管理システムScは、まず、少なくとも1つの利用権管理装置71と、少なくとも1つの機器81と、伝送

52

路91とを備えている。利用権管理装置71は、コンテンツ配信に関わる事業者α側に設置される。また、機器81は、事業者αとの契約に基づいてコンテンツ配信を受ける契約者β側に設置される。また、伝送路91は、有線伝送路または無線伝送路であり、利用権管理装置71および機器81をデータ通信可能に接続する。

【0182】次に、図55~図58を参照して、図54の利用権管理装置71および機器81の具体的な構成について説明する。図55は、図54の利用権管理装置71の詳細な構成を示す機能ブロック図である。図55において、利用権管理装置71は、コンテンツデータベース711と、復号鍵データベース712と、ユーザ情報データベース713と、利用権データベース714と、通信部715と、ユーザ認証部716と、利用権管理部717と、コンテンツ管理部718と、コンテンツ暗号化部719と、送信データ生成部720と、ライセンス情報生成部721と、復号鍵管理部722と、復号鍵暗号化部723とを備えている。

【0183】また、図56は、図55のライセンス情報生成部721の詳細な構成を示す図である。図56において、ライセンス情報生成部721は、ハッシュ値生成部7211と、ライセンス情報組立部7212とを含んでいる。

【0184】また、図57は、図54の機器81の詳細な構成を示す機能ブロック図である。図57において、機器81は、従前の実施形態と同様の民生機器であるが、本実施形態では、便宜上、音楽再生機であると仮定して、以降の説明を続ける。以上の仮定下では、機器81は、機器識別子格納部811と、設定要求生成部812と、通信部813と、コンテンツ管理部814と、コンテンツ蓄積部815と、発行要求生成部816と、ライセンス情報処理部817と、コンテンツ復号部818と、コンテンツ再生部819とを備えている。

【0185】また、図58は、図57のライセンス情報処理部817の詳細な構成を示す機能ブロック図である。図58において、ライセンス情報処理部817は、改竄判定部8171と、ハッシュ値生成部8172と、利用許可判定部8173と、復号鍵復号部8174とを含んでいる。

【0186】次に、上記ライセンス情報管理システムScにおいて、契約者βが事業者αからコンテンツ配信を受けるために必要となる準備について説明する。かかる準備作業では、図55のコンテンツデータベース(以下、コンテンツDBと称する)711と、復号鍵データベース(以下、復号鍵DBと称す)712と、ユーザ情報データベース(以下、ユーザ情報DB)713とが構築される。

【0187】まず、図59(a)を参照して、図55のコンテンツDB711について詳細に説明する。事業者αは、図59(a)に示すようなコンテンツDB711

を構築する。より具体的には、事業者 α は、契約者 β に提供すべきコンテンツデータDcntを、自分で作成したり、別のコンテンツ制作者から受け取る。ここで、コンテンツデータDcntは、機器81で利用可能なデータであって、例えば、テレビ番組、映画、ラジオ番組、音楽、書籍または印刷物を表す。また、コンテンツデータDcntは、ゲームプログラムまたはアプリケーションプログラムであっても良い。ただし、便宜上、本実施形態では、コンテンツデータDcntは音楽を表すデータであるとして、以下の説明を続ける。

【0188】事業者 α は、以上のようにして得たコンテンツデータDcntのそれぞれに、コンテンツ識別子Icntを割り当てる。コンテンツ識別子Icntとは、本ライセンス情報管理システムScにおいてコンテンツデータDcntを一意に特定する。また、以上のコンテンツデータDcntは、デジタルライツを保護する観点から、利用権管理装置71側で暗号化された上で機器81に配信される。そのため、事業者 α は、各コンテンツデータDcntに専用の暗号鍵Keを割り当てる。以上のコンテンツ識別子Icnt、コンテンツデータDcntおよび暗号鍵Keの組み合わせがコンテンツDB711に蓄積される。したがって、図59(a)に示すように、コンテンツDB711は、コンテンツ識別子Icnt、コンテンツデータDcntおよび暗号鍵Keの組み合わせの集まりとなる。コンテンツDB711において、コンテンツ識別子Icntは特に、同じ組みのコンテンツデータDcntを一意に特定する。また、暗号鍵Keは、同じ組みのコンテンツデータDcntを暗号化するために使用される。

【0189】なお、以下の説明の便宜のため、図59(a)に示す1つのコンテンツデータDcntには、一意なコンテンツ識別子Icntとしての「a」が割り当てられると仮定する。さらに、コンテンツ識別子Icntとしての「a」と同じ組みには、専用の暗号鍵Keとしての「b」が登録されると仮定する。

【0190】また、本実施形態では、コンテンツDB711は、コンテンツ識別子Icnt、コンテンツデータDcntおよび暗号鍵Keから構成されるが、コンテンツデータDcntおよび暗号鍵Ke毎のデータベースが構築されてもよい。また、コンテンツ識別子Icntは、コンテンツDB711におけるコンテンツデータDcntの格納場所を特定する場合がある。かかる場合には、コンテンツDB711に、コンテンツ識別子Icntを登録しておく必要性はない。つまり、コンテンツ識別子Icntは、コンテンツDB711に必須の構成要素とならない。

【0191】次に、図59(b)を参照して、図55の復号鍵DB712について詳細に説明する。上述したように、各コンテンツデータDcntは専用の暗号鍵Keで暗号化された状態で機器81に送信される。ここで、以下の説明において、暗号化されたコンテンツデータDcntを暗号済みコンテンツデータDecntと称する。暗号済

みコンテンツデータDecntの復号のために、暗号鍵Keに対応する復号鍵Kdが、機器81に提供される必要がある。そのため、事業者 α は、コンテンツDB711内の各暗号鍵Keに対応する復号鍵Kdを準備する。ここで、復号鍵Kdは、暗号鍵Keと同じビット列からなっているてもよいし、異なるビット列からなっているてもよい。以上の復号鍵Kdは、上述のコンテンツ識別子Icntと共に、復号鍵DB712に蓄積される。以上のことから、復号鍵DB712は、図59(b)に示すように、コンテンツ識別子Icntおよび復号鍵Kdの組み合わせの集まりとなる。復号鍵DB712において、コンテンツ識別子Icntは特に、同じ組みの復号鍵Kdに割り当てられているコンテンツデータDcntを特定する。また、復号鍵Kdは、同じ組みのコンテンツ識別子Icntで特定される暗号済みコンテンツデータDecntを復号するために使用される。

【0192】なお、以下の説明の便宜のため、図59(b)において、コンテンツ識別子Icntとしての「a」と同じ組みには、復号鍵Kdとしての「c」が登録されると仮定する。上述からも明らかであるが、復号鍵Kdとしての「c」は、暗号鍵Keとしての「b」による暗号済みコンテンツデータDecntの復号に使用される。

【0193】次に、図60(a)を参照して、図55のユーザ情報DB713について詳細に説明する。上述の契約者 β は、事業者 α からコンテンツ配信を受けるために契約を交わす。ここで、両者の契約に関しては、契約者 β が伝送路91を通じて事業者 α と行ってもよいし、他の形態で行ってもよい。この契約に基づいて、事業者 α は、契約者 β に機器識別子Idvを割り当てる。機器識別子Idvは、ライセンス情報管理システムScにおいて、契約者 β の機器81を一意に特定する。以上の機器識別子Idvが、ユーザ情報DB713に登録される。以上のことから、図60(a)に示すように、ユーザ情報DB713は、機器識別子Idvの集まりとなる。

【0194】ここで図57を再度参照する。図57に示すように、事業者 α により割り当てられた機器識別子Idvはさらに、契約者 β 側の機器81における機器識別子格納部811に設定される。機器識別子Idvの設定に関しては、典型的には、事業者 α が契約者 β 側で管理される機器81を操作して設定する。また、他にも、事業者 α 側が、伝送路91を通じて、契約者 β に割り当てた機器識別子Idvを送信し、機器81が、受信した機器識別子Idvを機器識別子格納部811に自動的に登録するようにしてもよい。

【0195】なお、以上の機器識別子Idvは、機器81の工場出荷時に予め、機器識別子格納部811に設定されているてもよい。このような場合、契約者 β は、事業者 α のコンテンツ配信に加入する際に、機器81に設定されている機器識別子Idvを当該事業者 α に告知する。そ

して、事業者αは、告知された機器識別子1dvをユーザ情報DB713に登録する。

【0196】なお、以下の説明の便宜のため、図60(a)に示すように、ユーザ情報DB713には、1つの機器識別子1dvとして「x1」が登録されると仮定する。また、図57に示すように、機器識別子格納部811には、機器識別子1dvとして「x1」が設定されると仮定する。

【0197】ここで、図60(b)には、利用権データベース714が示されているが、当該利用権データベース714については、後で説明する。

【0198】以上の準備が終了すると、機器81は、契約者βの操作に従って、利用権管理装置71から、コンテンツデータDcntを取得することが可能となる。以下、図61を参照して、コンテンツデータDcntの取得時における機器81および利用権管理装置71の動作について説明する。まず、契約者βは、機器81を操作して、利用権管理装置71にアクセスして、そのコンテンツDB711に蓄積されているコンテンツデータDcntの中から、今回取得したいもののコンテンツ識別子1cntを特定する。以降の説明において、今回指定されたコンテンツデータDcntを、取得対象コンテンツデータDcntと称する。さらに、契約者βは、取得対象コンテンツデータDcntを利用する際の利用条件Ccntを指定する。

【0199】以下、利用条件Ccntについて、より詳細に説明する。利用条件Ccntは、どのような条件で、機器81がコンテンツデータDcntの利用権の設定を要求するのかわかる情報である。コンテンツデータDcntが音楽を表す場合、利用条件Ccntとしては、有効期間、再生回数、最大連続再生時間、総再生時間または再生品質が代表的である。また、利用条件Ccntは、有効期間、再生回数、最大連続再生時間、総再生時間および再生品質の内、2つ以上の組み合わせであってもよい。利用条件Ccntとしての有効期間は、例えば、2001年6月1日から2001年8月31日までと設定され、設定された期間に限り、機器81は、コンテンツデータDcntを再生できる。再生回数は、例えば、5回と設定され、設定された回数に限り、機器81は、コンテンツデータDcntを再生できる。最大連続再生時間は、例えば、10秒と設定され、1回の再生において設定された時間までであれば、機器81は、コンテンツデータDcntを再生できる。このような最大連続再生時間は、音楽のプロモーションに特に有効である。総再生時間は、例えば、10時間と設定され、設定された時間の範囲内であれば、機器81は、コンテンツデータDcntを自由に再生できる。再生品質は、例えば、CD(CompactDisc)の品質と設定され、機器81は、設定された再生品質でコンテンツデータDcntを再生できる。

【0200】なお、上述では、コンテンツデータDcnt

が音楽を表す場合に設定される利用条件Ccntについて説明した。しかし、上述のみに限らず、利用条件Ccntは、コンテンツデータDcntが表す内容に応じて、適切に設定されることが好ましい。また、便宜上、本実施形態では、利用条件Ccntは、コンテンツデータDcntの再生回数であるとして、以下の説明を続ける。

【0201】上述したように、契約者βは、機器81を操作して、コンテンツ識別子1cntおよび利用条件Ccntを指定する。このような指定に回答して、機器81は、図62(a)に示す設定要求Drrを生成し、利用権管理装置71に送信する(図61;ステップS201)。設定要求Drrは、取得対象コンテンツデータDcntの利用権設定を利用権管理装置71に要求するための情報であるが、本実施形態ではさらに、取得対象コンテンツデータDcntの配信を利用権管理装置71に要求するための情報でもある。ステップS201をより具体的に説明すると、まず、設定要求生成部812(図57参照)は、契約者βが指定したコンテンツ識別子1cntおよび利用条件Ccntを受け取る。また、設定要求生成部812は、機器識別子格納部811から機器識別子1dvを受け取る。その後、設定要求生成部812は、以上の機器識別子1dv、コンテンツ識別子1cntおよび利用条件Ccntに、予め保持する設定要求識別子1rrを付加して、設定要求Drr(図62(a)参照)を生成する。ここで、設定要求識別子1rrは、利用権管理装置71が設定要求Drrを特定するために使用される。設定要求生成部812は、以上の設定要求Drrを通信部813に渡す。通信部813は、受け取った設定要求Drrを、伝送路91を通じて、利用権管理装置71に送信する。

【0202】利用権管理装置71(図55参照)において、通信部715は、伝送路91を通じて送信されてくる設定要求Drrを受信して、ユーザ認証部716に渡す。ユーザ認証部716は、設定要求Drrを受け取ると、ユーザ認証処理を行う(図61;ステップS202)。より具体的には、ユーザ認証部716は、上述のユーザ情報DB713(図60(a)参照)を管理しており、受け取った設定要求Drrに設定されている機器識別子1dvに一致するものが、当該ユーザ情報DB713に登録されているか否かを確認する。ユーザ認証部716は、ユーザ情報DB713に一致するものが登録されている場合に限り、今回設定要求Drrが、契約者βの機器81から送信されてきたものであると判断する。ユーザ認証部716は、以上のユーザ認証が終了すると、受け取った設定要求Drrを利用権管理部717に渡す。

【0203】なお、正規の契約者β以外からの設定要求Drrを受け取った場合、ユーザ認証部716は、ユーザ認証に失敗する。かかる場合、ユーザ認証部716は、当該設定要求Drrを利用権管理部717に渡すことなく、当該設定要求Drrを廃棄する。

【0204】利用権管理部717(図55参照)は、利

用権データベース（以下、利用権DBと称する）714を管理している。また、利用権管理部717は、そこに設定されている設定要求識別子1rrに基づいて、ユーザ認証部716から設定要求Drrを渡されたことを認識する。このような認識結果に従って、利用権管理部717は、利用権DB714への利用権登録処理を行う（ステップS203）。より具体的には、利用権管理部717は、設定要求Drrから、機器識別子1dv、コンテンツ識別子1cnt および利用条件Cntを取り出して、それらの組み合わせを利用権DB714に登録する。ここで、利用権管理部717は、設定要求Drrに設定されている利用条件Cntで、機器81が取得対象コンテンツデータDcntを利用する権利を要求しているとみなす。つまり、利用権管理部717からみれば、利用条件Cntは、取得対象コンテンツデータDcntを機器81が利用できる権利を示す。以上の観点から、利用権管理部717は、設定要求Drrから取り出した利用条件Cntを、機器81が設定要求している利用権情報Dratとして扱う。つまり、利用権DB714は、図60（b）に示すように、機器識別子1dv、コンテンツ識別子1cnt および利用権情報Dratの組み合わせの集まりとなる。これによって、利用権管理部717は、契約者β毎に、取得対象コンテンツデータDcntの利用権を管理する。利用権管理部717は、以上の利用条件登録処理が終了すると、今回受け取った設定要求Drrをコンテンツ管理部718に渡す。

【0205】ここで、以上の利用権DB714に登録される利用権情報Dratの具体例について説明する。既に説明している通り、本実施形態では、利用条件Cntは利用回数であると仮定されている。さらに、今回の設定要求Drrには、機器識別子1dvとして「x1」、コンテンツ識別子1cntとして「a」および利用条件Cntとして「再生m回」（mは自然数）が設定されていると仮定する。以上の仮定下では、図60（b）に示すように、機器識別子1dvとしての「x1」、コンテンツ識別子1cntとしての「a」および利用権情報Dratとしての「再生m回」の組み合わせが設定される。

【0206】なお、本ライセンス情報管理システムScの技術的特徴とは関係ないが、ステップS203において、利用権管理部717は、利用権情報Dratの登録毎に、機器識別子1dvが割り当てられている契約者βに対して課金を行ってもよい。

【0207】コンテンツ管理部718は、設定要求Drrを受け取ると、コンテンツデータDcntの読み出し処理を行う（ステップS204）。より具体的には、コンテンツ管理部718は、受け取った設定要求Drrから、コンテンツ識別子1cntを取り出す。その後、コンテンツ管理部718は、コンテンツDB711にアクセスして、取り出したコンテンツ識別子1cntが割り当てられているコンテンツデータDcnt および暗号鍵Keを読み

出す。以上の読み出し処理が終了すると、コンテンツ管理部718は、読み出したコンテンツデータDcnt および暗号鍵Keをコンテンツ暗号化部719に渡す。さらに、コンテンツ管理部718は、受け取った設定要求Drrを送信データ生成部720に渡す。

【0208】コンテンツ暗号化部719は、コンテンツデータDcntの暗号処理を行う（ステップS205）。より具体的には、コンテンツ暗号化部719は、受け取ったコンテンツデータDcntを、それと同時に受け取った暗号鍵Keで暗号化して、前述の暗号済みコンテンツデータDecntを生成する。コンテンツ暗号化部719は、以上の暗号処理が終了すると、暗号済みコンテンツデータDecntを送信データ生成部720に渡す。

【0209】送信データ生成部720は、コンテンツ管理部718からの設定要求Drrと、コンテンツ暗号化部719からの暗号済みコンテンツデータDecntとが揃うと、送信データ生成処理を行う（ステップS206）。より具体的には、送信データ生成部720は、受け取った設定要求Drrから、コンテンツ識別子1cntを取り出す。さらに、送信データ生成部720は、取り出したコンテンツ識別子1cntを、受け取った暗号済みコンテンツデータDecntに付加して、図62（b）に示すような、送信データDtrnを生成する。送信データ生成部720は、以上の送信データ生成処理が終了すると、送信データDtrnを通信部715に渡す。通信部715は、受け取った送信データDtrnを、伝送路91を介して、機器81へと送信する（ステップS207）。

【0210】機器81（図57参照）において、通信部813は、伝送路91を通じて送信されてくる送信データDtrnを受信する（ステップS208）。より具体的には、通信部813は、それに含まれるコンテンツ識別子1cntから、今回、送信データDtrnを受信したことを認識する。このような認識結果に従って、通信部813は、受信データDtrnをコンテンツ管理部814に渡す。

【0211】コンテンツ管理部814は、受信データDtrn内のコンテンツ識別子1cnt および暗号済みコンテンツデータDecntを、コンテンツ蓄積部815に蓄積する（ステップS209）。つまり、コンテンツ蓄積部815には、図63に示すように、上述の設定要求Drrにより要求されたコンテンツ識別子1cnt および暗号済みコンテンツデータDecntの組み合わせが、いくつか蓄積されることになる。

【0212】デジタルライツの保護の観点から、機器81には暗号済みコンテンツデータDecntが配信される。そのため、機器81は、コンテンツデータDcntを利用する場合には、利用権管理装置71により提供される復号鍵Kdで、暗号済みコンテンツデータDecntを復号する必要がある。ここで、本ライセンス情報管理システムScでは、復号鍵Kdを機器81に提供するために、後

で詳説するライセンス情報D1cが用いられる。以下、図64～図66を参照して、ライセンス情報D1cの取得およびコンテンツデータDcntの復号時における機器81および利用権管理装置71の動作について説明する。

【0213】まず、契約者8は、機器81を操作して、コンテンツ蓄積部815にアクセスして、そこに蓄積されている暗号済みコンテンツデータDecntの中から、今回利用したいものを特定する。ここで、以下の説明において、今回指定された暗号済みコンテンツデータDecntを、復号対象コンテンツデータDecntと称する。

【0214】以上の契約者8による指定に回答して、機器81は、図67(a)に示すような発行要求Dirを生成し、利用権管理装置71に送信する(図64:ステップS301)。発行要求Dirは、上述のライセンス情報D1cの提供を利用権管理装置71に要求するため、つまり復号対象コンテンツデータDecntの利用許可を受けるための情報である。より具体的にステップS301を説明すると、コンテンツ管理部814(図57参照)は、コンテンツ蓄積部815を管理しており、契約者8により特定された復号対象コンテンツデータDecntに付加されているコンテンツ識別子Icntを、当該コンテンツ蓄積部815から取り出す。発行要求生成部816は、コンテンツ管理部814により取り出されたコンテンツ識別子Icntを受け取る。さらに、発行要求生成部816は、機器識別子格納部811から機器識別子I dvを受け取る。その後、発行要求生成部816は、機器識別子I dvおよびコンテンツ識別子I cntに、発行要求識別子I irを付加して、発行要求Dir(図67(a)参照)を生成する。ここで、発行要求識別子I irは、利用権管理装置71が発行要求Dirを特定するために使用される。発行要求生成部816は、以上の発行要求Dirを通信部813に渡す。通信部813は、受け取った発行要求Dirを伝送路91を通じて、利用権管理装置71に送信する。

【0215】利用権管理装置71において、通信部715(図55参照)は、伝送路91を通じて送信されてくる発行要求Dirを受信して、ユーザ認証部716に渡す。

【0216】ユーザ認証部716は、発行要求Dirを受け取ると、ユーザ認証処理を行う(ステップS302)。より具体的には、ユーザ認証部716は、受け取った発行要求Dirから、機器識別子I dvを取り出す。この後、ユーザ認証部716は、ステップS202(図61参照)と同様にして、今回の発行要求Dirに認証処理を行った後に、当該発行要求Dirを利用権管理部717に渡す。

【0217】利用権管理部717は、それに設定されている発行要求識別子I irに基づいて、今回、ユーザ認証部716から発行要求Dirを渡されたことを認識する。このような認識結果に従って、利用権管理部717は、

受け取った発行要求Dirから、機器識別子I dvおよびコンテンツ識別子I cntを取り出す(ステップS303)。次に、利用権管理部717は、取り出した機器識別子I dvおよびコンテンツ識別子I cntの組み合わせが、利用権DB714(図60(b)参照)に登録されているか否かを判断する(ステップS304)。

【0218】利用権管理部717は、ステップS304で「Yes」と判断した場合、それらと同じ組みの利用権情報D ratを参照して、機器81に利用許可を与えることができるか否かを判断する(ステップS305)。ステップS305で「Yes」と判断した場合、利用権管理部717は、利用権情報D ratの一部または全てを取り出す(ステップS306)。ここで、以下の説明において混同が生じることを避けるため、ステップS306において取り出された一部または全ての利用権情報D ratのことを、今回の発行要求Dirにより特定される機器81にコンテンツデータDcntの利用を許可するための情報であるという観点から、利用許可情報D lwと称する。つまり、ステップS306では、利用許可情報D lwが生成される。

【0219】利用許可情報D lwの生成により、機器81のために登録されている利用権情報D ratの一部または全てが使用される。そのため、ステップS306の次に、利用権管理部717は、ステップS306で一部または全部が取り出された利用権情報D ratを更新する(ステップS307)。

【0220】ここで、以上のステップS303～S307の処理の具体例について説明する。今、利用権DB714には、図60(b)に示すように、機器識別子I dvとしての「x1」、コンテンツ識別子I cntとしての「a」および利用権情報D ratとしての「再生m回」の組みが登録されていると仮定する。また、今回、機器81は、機器識別子I dvとしての「x1」およびコンテンツ識別子I cntとしての「a」が設定されている発行要求Dirを送信すると仮定する。

【0221】以上の仮定下では、ステップS303において、発行要求Dirから、機器識別子I dvとしての「x1」と、コンテンツ識別子I cntとしての「a」が取り出される。また、ステップS304において、機器識別子I dvとしての「x1」およびコンテンツ識別子I cntとしての「a」の組みが、利用権DB714に登録されていると判断される。このように判断されると、ステップS305において、同じ組みの利用権情報D ratには、「再生m回」と設定されているので、機器81の利用許可を与えてもよいと判断される。このように判断されると、ステップS306において、利用許可情報D lwが生成される。この時生成される利用許可情報D lwとしては、例えば、「再生n回」が挙げられる。ここで、nは、上述のmを超えない自然数であり、より好ましくは、機器81の処理能力に応じて設定される。例えば、

機器81が相対的に低い性能のハードウェアを搭載している場合であれば、 n は、「1」のように、機器81が復号対象コンテンツデータDecntを利用可能な最低限の値に設定されることが好ましい。

【0222】以上のステップS303～S306により、機器81（機器識別子I dv「x1」）がコンテンツデータDcnt（コンテンツ識別子I cnt「a」）を再生する権利を n 回使うことになる。そのため、ステップS307において、利用権情報D rqt が「再生 m 回」から「再生（ $m-n$ ）回」に更新される。

【0223】以上の具体例では、利用権情報D rqt がコンテンツデータDcntの再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムScでは、様々な利用権情報D rqt（つまり利用条件Cnt）を設定することができる。従って、ステップS303からS307までの処理手順は、利用権情報D rqtに応じて適切に規定される必要がある。

【0224】以上のようにして生成した利用許可情報D lwを、利用権管理部717（図55参照）は、発行要求Dirと一緒に、ライセンス情報生成部721に渡す。より具体的には、ライセンス情報生成部721は、図56に示すように、ハッシュ値生成部7211およびライセンス情報組立部7212を含んでいる。ハッシュ値生成部7211には、利用許可情報D lwのみが渡され、また、ライセンス情報組立部7212には、利用許可情報D lwおよび発行要求Dirの双方が渡される。

【0225】まず、ハッシュ値生成部7211は、予め保持するハッシュ関数 $f(x)$ に、受け取った利用許可情報D lwを代入して、利用許可情報D lwの改竄を防止するためのハッシュ値V hsを生成する（ステップS308）。つまり、ハッシュ値V hsは、利用許可情報D lwを生成多項式 $f(x)$ に代入した時に得られる解である。以上のようなハッシュ値V hsを、ハッシュ値生成部7211は、ライセンス情報組立部7212に渡す。

【0226】ライセンス情報組立部7212は、受け取った発行要求Dirを復号鍵管理部722に渡す。復号鍵管理部722（図55参照）は、前述した復号鍵DB712（図59（b）参照）を管理する。復号鍵管理部722は、受け取った発行要求Dirに設定されているコンテンツ識別子I cnt および機器識別子I dvを取り出す。さらに、復号鍵管理部722は、コンテンツ識別子I cntと同じ組みの復号鍵K dを復号鍵DB712から取り出して、機器識別子I dvと一緒に復号鍵暗号化部723に渡す。復号鍵暗号化部723は、受け取った復号鍵K dを、同時に受け取った機器識別子I dvで暗号化して（ステップS309）、暗号済みの復号鍵K edを生成する。以上の暗号済み復号鍵K edは、ライセンス情報組立部7212に渡される。

【0227】ライセンス情報組立部7212は、発行要求Dirおよび利用許可情報D lw、ハッシュ値V hsならび

に暗号済み復号鍵K edのすべてが揃うと、図67（b）に示すライセンス情報D lcの生成を開始する（図65：ステップS3010）。より具体的には、ライセンス情報組立部7212は、発行要求Dirから、コンテンツ識別子I cntを取り出して、利用許可情報D lw、暗号済み復号鍵K edおよびハッシュ値V hsに付加する。さらに、ライセンス情報組立部7212は、予め保持するライセンス情報識別子I lcを、コンテンツ識別子I cntに付加して、ライセンス情報D lcを生成する。以上のライセンス情報D lcは、復号対象コンテンツデータDecntの機器81における利用を制御するための情報である。また、ライセンス情報識別子I lcは、機器81がライセンス情報D lcを特定するための情報である。また、以上のライセンス情報D lcは、通信部715に渡される。通信部715から、伝送路91を通じて、機器81に送信される（ステップS3011）。

【0228】機器81（図57参照）において、通信部813は、伝送路91を通じて送信されてくるライセンス情報D lcを受信する（ステップS3012）。より具体的には、通信部813は、それに設定されるライセンス情報識別子I lcから、今回、ライセンス情報D lcを受け取ったことを認識する。このような認識結果に従って、通信部813は、受け取ったライセンス情報D lcをライセンス情報処理部817に渡す。

【0229】ライセンス情報処理部817は、図58に示すように、改竄判定部8171と、ハッシュ値生成部8172と、利用許可判定部8173と、復号鍵復号部8174とを含んでいる。通信部813からのライセンス情報D lcは、まず、改竄判定部8171に渡される。改竄判定部8171は、まず、受け取ったライセンス情報D lcから、利用許可情報D lwおよびハッシュ値V hsを取り出し（ステップS3013）、取り出した利用許可情報D lwを、ハッシュ値生成部8172に渡し、ハッシュ値V hsをそのまま保持する。ここで、以下の説明において混同が生じないように、ステップS3013で取り出されたハッシュ値V hsを、機器81の外部（つまり利用権管理装置71）で生成されたものであるという観点から、外部ハッシュ値V ehsと称する。

【0230】ハッシュ値生成部8172は、利用権管理装置71側のハッシュ値生成部7211（図3参照）と同じハッシュ関数 $f(x)$ を保持しており、受け取った利用許可情報D lwをハッシュ関数 $f(x)$ に代入してハッシュ値V hsを生成する（ステップS3014）。ここでステップS3014で生成されたハッシュ値V hsを、機器81の内部で生成されたものであるという観点から、内部ハッシュ値V lhsと称する。ハッシュ値生成部8172は、以上の内部ハッシュ値V lhsを、改竄判定部8171に返す。

【0231】改竄判定部8171は、上述の内部ハッシュ値V lhsを受け取ると、利用許可情報D lwが改竄され

ているか否かを判定する（ステップS3015）。より具体的には、上述の内部ハッシュ値V1hsは、ライセンス情報D1c内の利用許可情報D1wが改竄されていないという条件で、外部ハッシュ値Vehsに一致する。そこで、ステップS3015において、改竄判定部8171は、受け取った内部ハッシュ値V1hsが外部ハッシュ値Vehsに一致するか否かを判定する。改竄判定部8171は、「Yes」と判定した場合には、利用許可情報D1wが改竄されておらず、今回送信されてきた利用許可情報D1wが有効であるとみなして、今回受け取ったライ

10 センス情報D1cを利用許可判定部8173に渡す。
 【0232】利用許可判定部8173は、受け取ったライセンス情報D1cを参照して、復号対象コンテンツデータDecntの利用が許可されているか否かを判定する（ステップS3016）。利用許可判定部8173は、ステップS3016において「Yes」と判断した場合に限り、受け取ったライセンス情報D1cから、暗号済み復号鍵Kedを取り出して、復号鍵復号部8174に渡す。

20 【0233】ここで、以上のステップS3016の処理の具体例について説明する。前述の仮定に従えば、今回のライセンス情報D1cの利用許可情報D1wにより、コンテンツデータDecntの再生がn回だけ許可されている。かかる場合、利用許可判定部8173は、ステップS3016において、利用許可情報D1wに設定される再生回数が1以上であれば、復号対象コンテンツデータDecntの利用が許可されていると判断して、受け取ったライセンス情報D1cから暗号済み復号鍵Kedを取り出して、復号鍵復号部8174に渡す。

30 【0234】以上の具体例では、利用権情報DratがコンテンツデータDecntの再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムScでは、様々な利用権情報Drat（つまり利用条件Cnt）を設定することができる。従って、ステップS3016の処理は、利用権情報Dratに応じて適切に規定される必要がある。

40 【0235】さて、復号鍵復号部8174は、利用許可判定部8173から暗号済み復号鍵Kedを受け取る。さらに、復号鍵復号部8174は、機器識別子格納部811から機器識別子Idvを受け取る。その後、復号鍵復号部8174は、暗号済み復号鍵Kedを、機器識別子Idvで復号して（ステップS3017）、復号鍵Kdをコンテンツ復号部818に渡す。

50 【0236】ところで、コンテンツ管理部814は、ステップS301において、コンテンツ識別子Icntだけでなく、前述の復号対象コンテンツデータDecntを取り出す。取り出された復号対象コンテンツデータDecntは、コンテンツ復号部818に渡される。コンテンツ復号部818は、復号鍵復号部8174から受け取った復号鍵Kdで、復号対象コンテンツデータDecntを復号して（ステップS3018）、コンテンツデータDecntを

コンテンツ再生部819に渡す。コンテンツ再生部819は、受け取ったコンテンツデータDecntを再生して、音声出力する（ステップS3019）。これにより、契約者Bは、事業者Aから購入したコンテンツデータDecntが表す音楽を聴くことができる。

【0237】ここで、図65のステップS3015を参照する。ステップS3015において、改竄判定部8171は、利用許可情報D1wが改竄されていると判定する場合がある。また、ステップS3016において、利用許可判定部8173は、復号対象コンテンツデータDecntの利用が許可されていないと判定する場合もある。このような場合、改竄判定部8171および利用許可判定部8173は、今回受け取ったライセンス情報D1cを破棄する（図66；ステップS3020）。以上から明らかのように、本ライセンス情報管理システムScでは、有効なライセンス情報D1cを受信した場合にのみ、復号対象コンテンツデータDecntの復号が許可される。これによって、上述のデジタルライツが保護される。

【0238】ここで、図64のステップS304において、利用権管理部717は、機器識別子Idvおよびコンテンツ識別子Icntの組み合わせが、利用権DB714（図60（b）参照）に登録されていないと判断する場合がある。さらに、ステップS305において、利用権管理部717は、機器81に利用許可を与えないと判断する場合もある。このような場合、利用権管理部717は、復号対象コンテンツデータDecntの利用を拒否することを示す利用拒否情報Drij（図67（c）参照）を生成して、通信部715に渡す。通信部715は、受け取った利用拒否情報Drijを、伝送路91を介して、機器81に送信する（図66；ステップS3021）。

【0239】機器81（図57参照）において、通信部813は、伝送路91を通じて送信されてくる利用拒否情報Drijを受信する（ステップS3022）。利用拒否情報Drijの受信以降、機器81では何の処理も行われない。以上から明らかのように、本ライセンス情報管理システムScでは、利用権DB714に有効な機器識別子Idv、コンテンツ識別子Icntおよび利用権情報Dratの組み合わせが登録されていない場合には、利用拒否情報Drijが機器81に送信される。これによって、機器81側では、復号対象コンテンツデータDecntは復号されない。これによって、上述のデジタルライツが保護される。

【0240】なお、ステップS304において、利用権管理部717は、機器識別子Idvおよびコンテンツ識別子Icntの組み合わせが、利用権DB714（図60（b）参照）に登録されていないと判断する場合、機器識別子Idv、コンテンツ識別子Icntおよび利用権情報Dratの組み合わせを新しく生成して、当該利用権DB714に登録するようにしてもよい。

【0241】以上説明したように、本ライセンス情報管

理システムScでは、各コンテンツデータDcntを機器81が利用するための権利を表す利用権情報Dratを利用権管理装置71側で一元的に管理できるようになる。そのため、以上のような利用権情報Dratを管理するための処理負担を機器81に負わせる必要がなくなる。これによって、本ライセンス情報管理システムScによれば、処理能力の低い民生機器に適した権利保護技術を提供することができる。

【0242】なお、以上の実施形態では、同じ事業者αにより管理される利用権管理装置71が、図61の処理および図64～図66の処理の双方を行うとして説明した。しかしながら、互いに異なる利用権管理装置が図61の処理と図64～図66の処理とを行うようにしてもよい。つまり、ある事業者により管理される利用権管理装置がコンテンツデータDcntの配信を担当し、他の事業者により管理される利用権管理装置がライセンス情報D1cの提供を担当するように、本ライセンス情報管理システムScは構成されてもよい。さらに、説明の便宜のため、本実施形態では、最初に、コンテンツデータDcntの取得（図61の処理）が行われ、その後、ライセンス情報D1cの取得（図64～図66の処理）が行われていた。しかしながら、最初にライセンス情報D1cの取得が行われ、その後、コンテンツデータDcntの取得が行われてもよい。また、コンテンツデータDcntの取得およびライセンス情報D1cの取得が同時並行して行われてもよい。

【0243】また、以上の実施形態では、コンテンツDB114は、暗号化されていないコンテンツデータDcntおよび暗号鍵Keの集まりであった。利用権管理装置71は、送信データDtrmの生成直前に、コンテンツデータDcntを暗号鍵Keで暗号化するようにしていた（ステップS205参照）。しかしながら、コンテンツデータDcntの暗号化に要する処理時間を削減するために、コンテンツDB114は、前述の暗号済みコンテンツデータDecntの集まりであってもよい。この場合、利用権管理装置71は、設定要求Drrに設定されるコンテンツ識別子Icntが示す暗号済みコンテンツデータDecntに、当該コンテンツ識別子Icntを付加して送信データDtrmを生成し送信する。

【0244】また、以上の実施形態では、ライセンス情報生成部721において、ハッシュ値生成部7211は、利用許可情報D1wのみからハッシュ値Vhsを生成していた。しかし、これに限らず、以下のようにしてハッシュ値Vhsを生成してもよい。まず、ライセンス情報組立部7212は、ライセンス情報D1cの構成要素であるライセンス情報識別子I1c、コンテンツ識別子Icnt、利用許可情報D1w、および暗号済み復号鍵Kedの内いずれか、もしくは2つ以上をハッシュ値生成部7211に渡す。ハッシュ値生成部7211は、ライセンス情報組立部7212から受け取ったものを、上述のハッシュ

関数 $f(x)$ に代入して、ハッシュ値Vhsを生成する。

【0245】また、以上の実施形態では、ライセンス情報D1cは、暗号済み復号鍵Kedを含んでいた。しかし、これに限らず、ライセンス情報D1cは、復号鍵Kdを含んでいてもよい。この場合、伝送路91上で、第三者に復号鍵Kdが盗まれる危険があるので、SSL(Secure Socket Layer)に代表される技術を用いて、利用権管理装置71から機器81へと伝送されるライセンス情報D1cを保護することが好ましい。さらに、SSLだけでは、機器81において、ライセンス情報D1cがそのままの状態で保持される。このような状況では、機器81から他の機器へとライセンス情報D1cが転送されれば、当該他の機器は、ライセンス情報D1cを利用できるので、デジタルライツの保護という観点からは好ましくない。そのため、機器識別子格納部811に格納される機器識別子I1dvでライセンス情報D1cを暗号化するアルゴリズムを、機器81に組み込むことがより好ましい。これにより、ライセンス情報D1cは機器81以外では使用できなくなるので、デジタルライツを保護することが可能となる。

【0246】また、以上の実施形態では、説明の便宜上、ユーザ情報DB713には、機器識別子I1dvのみが登録されるとして説明した。しかしながら、ユーザ情報DB713にはさらに、契約者βを一意に特定可能な他のユーザ情報（例えば、住所および電話番号）が登録されてもよい。また、以上のような複雑なユーザ情報で復号鍵Kdを暗号化するようにしてもよい。これによって、復号鍵Kdの暗号強度が高くなるので、より好ましくデジタルライツを保護できるライセンス情報管理システムScを提供することが可能となる。

【0247】また、以上の実施形態では、説明の便宜上、コンテンツデータDcntが音楽データであるとして説明した。そのため、機器81は、コンテンツ再生部819を含んでおり、当該コンテンツ再生部819は、復号されたコンテンツデータDcntを再生して、音声出力するとして説明した。しかしながら、前述したように、コンテンツデータDcntは、機器81で利用可能なデータであればよく、当該コンテンツデータDcntが表すのは、テレビ番組、映画、ラジオ番組、書籍、印刷物、ゲームプログラムまたはアプリケーションプログラム等、多岐にわたる。したがって、コンテンツ再生部819は、音声出力するものに限らず、コンテンツデータDcntの種類に応じて、テレビ番組、映画、書籍および印刷物およびゲーム内容を映像出力可能なもの、ラジオ番組を音声出力可能なものに置換されてもよい。さらに、機器81は、以上のようなコンテンツ再生部819に代えて、復号されたコンテンツデータDcntを、外部の機器（テレビジョン受像機、ラジオ受信機、音楽再生機、電子ブックリーダー、ゲーム機器、PC、情報携帯端末、携帯電話、外部記憶装置等）に転送可能なインター

フェイスを備えていてもよい。

【0248】ところで、以上のライセンス情報管理システムScにおいて、事業者αは、契約者βにコンテンツ配信を提供する。しかしながら、上述のライセンス情報管理システムScでは、機器81に機器識別子Idvが固定的に設定されてしまうため、契約者βが、同じ事業者αと契約している宿泊施設において、自分の利用権情報Drqtを使ってコンテンツデータDcntを、当該宿泊施設に設置された機器81で利用することができないという問題点があった。また、同様の理由で、ある契約者βが、同じ事業者αと契約している知人宅において、自分の利用権情報Drqtを使って、コンテンツデータDcntを利用することができないという問題点があった。以下の第6の変形例に係るライセンス情報管理システムSc1は、以上のような問題点を解決して、より使い勝手のよいコンテンツ配信を実現することを目的とする。

【0249】「第6の変形例」図68は、ライセンス情報管理システムSc1の全体構成を示すブロック図である。図68のライセンス情報管理システムSc1は、図54のライセンス情報管理システムScと比較すると、可搬型記録媒体101および機器201とをさらに備える点で相違する。この点以外に両システムScおよびSc1の間に構成面での相違は無いので、図68において、図54のライセンス情報管理システムScに相当する構成には同一の参照符号を付し、その説明を簡素化する。つまり、以下において、利用権管理装置71および機器81の説明を行う場合には、図55～図57を援用する。

【0250】可搬型記録媒体101は、代表的には、SDカードやスマートメディア（いずれも商標）のように、契約者βが携帯可能な種類の記録媒体であって、図69に示すように、自身を一意に特定するメディア識別子Imdを、予め定められた記録領域に格納している。ここで、本実施形態では、便宜上、図69に示すように、メディア識別子Imdは「x2」であるとして、以下の説明を続ける。以上の可搬型記録媒体101は、前述の機器81と同じ契約者βにより管理される。

【0251】機器201は、事業者αとの契約に基づいてコンテンツ配信を受ける契約者γ側に設置される。ここで、契約者γは、本実施形態では、上述したような宿泊施設を所有しており、機器201は、当該宿泊施設に設置される。以下、機器201の詳細な構成を説明する。

【0252】ここで、図70は、図68の機器201の詳細な構成を示す機能ブロック図である。図70において、機器201は、機器81と同様の民生機器が代表的であるが、本実施形態では、便宜上、音楽再生機であると仮定して、以降の説明を続ける。以上の仮定下では、機器201は、上述の可搬型記録媒体101を装着可能に構成されており、図57に示す機器81と比較すると、インターフェイス2021と、識別子抽出部202

2とをさらに備える点で相違する。この点以外に両機器201および81の間に構成面での相違は無いので、図70の機器201において、図57の機器81に相当する構成には同一の参照符号を付し、その説明を簡素化する。

【0253】次に、上記ライセンス情報管理システムSc1において、契約者βが、自分の利用権情報Drqtを使って、他者（つまり、契約者γ）側の機器201上で事業者αからコンテンツ配信を受けるために必要となる準備について説明する。かかる準備作業では、前述の実施形態と同様に、まず、図55のコンテンツデータベース（以下、コンテンツDBと称する）711と、復号鍵データベース（以下、復号鍵DBと称す）712と、ユーザ情報データベース（以下、ユーザ情報DB）713とが構築される。なお、コンテンツDB711および復号鍵DB712については、図59（a）および同図（b）を参照して前述した通りであるため、本変形例では、それぞれの説明を省略する。

【0254】しかしながら、ユーザ情報DB713には、前述の実施形態とは異なる情報の組み合わせが登録される。次に、図71（a）を参照して、図55のユーザ情報DB713について詳細に説明する。上述の契約者βは、事業者αからコンテンツ配信を受けるために契約を交わす。この契約に基づいて、事業者αは、契約者βにユーザ識別子Iusrを割り当てる。ここで、ユーザ識別子Iusrは、契約者βを一意に特定する。さらに、事業者αは、契約者βが管理する機器81に、前述と同様の機器識別子Idvを割り当てる。なお、上述の実施形態で説明したように、契約者βが、予め機器81に設定されている機器識別子Idvを事業者αに告知してもよい。機器識別子Idvは、ライセンス情報管理システムSc1において、契約者βの機器81を一意に特定する。さらに、事業者αは、契約者βの可搬型記録媒体101に記録されているメディア識別子Imdの告知を受ける。以上の機器識別子Idvおよびメディア識別子Imdの組み合わせが、契約者βのために、ユーザ識別子Iusrと共に、ユーザ情報DB713に登録される。以上のことから、図71（a）に示すように、ユーザ情報DB713は、ユーザ識別子Iusr毎に登録される機器識別子Idvおよびメディア識別子Imdの組み合わせの集まりとなる。

【0255】また、前述の実施形態でも説明したように、事業者αにより割り当てられた機器識別子Idvはさらに、契約者β側の機器81における機器識別子格納部811に設定される（図57参照）。

【0256】また、上述の契約者γも、事業者αからコンテンツ配信を受けるために契約を交わす。ここで、説明の便宜のため、契約者γは、契約者βとは異なり、可搬型記録媒体101を所有していないとする。以上の契約に基づいて、事業者αは、契約者γに、一意なユーザ

識別子 Iusr を割り当てる。さらに、事業者 α は、契約者 γ の機器 201 に、ライセンス情報管理システム Sc1 において一意な機器識別子 Idv を割り当てる。以上の機器識別子 Idv が、契約者 γ のために、ユーザ情報 DB 713 に、ユーザ識別子 Iusr と共に登録される。以上のことから、図 71(a) に示すように、ユーザ情報 DB 713 は、ユーザ識別子 Iusr 毎に登録される機器識別子 Idv の集まりとなる。

【0257】また、事業者 α により、機器 201 に割り当てられた機器識別子 Idv は、図 70 に示すように、契約者 γ 側の機器 201 における機器識別子格納部 811 に設定される。

【0258】なお、以下の説明の便宜のため、図 71(a) に示すように、ユーザ情報 DB 713 には、契約者 β のために、ユーザ識別子 Iusr としての「y1」に対応して、機器識別子 Idv として「x1」およびメディア識別子 Imd として「x2」が登録されると仮定する。この仮定下では、図 57 に示すように、機器 81 側の機器識別子格納部 811 には、機器識別子 Idv として「x1」が設定される。さらに、ユーザ情報 DB 713 には、契約者 γ のために、ユーザ識別子 Iusr としての「y2」に対応して、機器識別子 Idv として「x3」が登録されると仮定する。この仮定下では、図 70 に示すように、機器 201 側の機器識別子格納部 811 には、機器識別子 Idv として「x3」が設定される。

【0259】ここで、図 71(b) には、利用権データベース 714 が示されているが、当該利用権データベース 714 については、後で説明する。

【0260】以上の準備が終了すると、機器 81 は、前述の実施形態で説明したように、利用権管理装置 71 から、コンテンツデータ Dcnt およびライセンス情報 Dlc を取得することが可能となる(図 61、図 64～図 66 参照)。さらに、本変形例の特徴的な点は、図 68 に示すように、契約者 β が可搬型記録媒体 101 を契約者 γ 側に持っていき、当該契約者 γ 側の機器 201 を使って、コンテンツデータ Dcnt およびライセンス情報 Dlc の提供を、利用権管理装置 71 から受けることができる点である。

【0261】以下、図 72 および図 73 を参照して、契約者 β が機器 201 を使ってコンテンツデータ Dcnt を取得する際における当該機器 201 および利用権管理装置 71 の動作について説明する。まず、契約者 β は、契約者 γ 側の機器 201 に、自分の可搬型記録媒体 101 を装着する。これによって、可搬型記録媒体 101 は、インターフェイス 2021 (図 70 参照) を通じて、識別子抽出部 2022 とデータ通信可能に接続される。その後、契約者 β は、機器 201 を操作して、利用権管理装置 71 にアクセスして、そのコンテンツ DB 711 に蓄積されているコンテンツデータ Dcnt の中から、今回取得したいもののコンテンツ識別子 Icnt を特定する。

以降の説明において、今回指定されたコンテンツデータ Dcnt を、取得対象コンテンツデータ Dcnt と称する。さらに、契約者 β は、取得対象コンテンツデータ Dcnt を利用する際の利用条件 Ccnt を指定する。ここで、利用条件 Ccnt については、前述の実施形態で詳しく説明しているので、ここではその説明を控える。また、本変形例においても、便宜上、利用条件 Ccnt は、コンテンツデータ Dcnt の再生回数であると仮定する。

【0262】上述したように、契約者 β は、機器 201 を操作して、コンテンツ識別子 Icnt および利用条件 Ccnt を指定する。設定要求生成部 812 (図 70 参照) は、契約者 β が指定したコンテンツ識別子 Icnt および利用条件 Ccnt を受け取る(ステップ S401)。

【0263】次に、設定要求生成部 812 は、識別子抽出部 2022 に、機器識別子 Idv およびメディア識別子 Imd のいずれか一方を選択して、自身に返すように指示する。ところで、可搬型記録媒体 101 が機器 201 に装着されている場合、当該機器 201 には、機器識別子格納部 811 に格納されている機器識別子 Idv と、可搬型記録媒体 101 に格納されているメディア識別子 Imd とが存在することになる。そのため、識別子抽出部 2022 は、設定要求生成部 812 の指示に回答して、可搬型記録媒体 101 が装着されている場合には、インターフェイス 2021 を通じて、当該可搬型記録媒体 101 に格納されているメディア識別子 Imd を取り出す。設定要求生成部 812 は、識別子抽出部 2022 により取り出されたメディア識別子 Imd を受け取る(ステップ S402)。

【0264】ここで、識別子抽出部 2022 は、機器 201 に可搬型記録媒体 101 が装着されていない場合、機器識別子格納部 811 から、機器識別子 Idv を取り出して、設定要求生成部 812 に渡すことになる。しかし、この場合、契約者 γ が、機器 201 を使って、コンテンツデータ Dcnt の取得を行うこととなる。このような場合については、本変形例の目的とは関係なく、さらには、識別子抽出部 2022 が機器識別子 Idv を取り出す場合における、機器 201 における動作については、前述の実施形態の説明から明らかであるため、その説明を省略する。

【0265】設定要求生成部 812 は、以上のメディア識別子 Imd、コンテンツ識別子 Icnt および利用条件 Ccnt に、予め保持する設定要求識別子 Irr を付加して、設定要求 Drr (図 74(a) 参照) を生成する(ステップ S403)。設定要求 Drr は、取得対象コンテンツデータ Dcnt の利用権設定を利用権管理装置 11 に要求するための情報であるが、本実施形態ではさらに、取得対象コンテンツデータ Dcnt の配信を利用権管理装置 71 に要求するための情報である。また、設定要求識別子 Irr は、利用権管理装置 71 が設定要求 Drr を特定するために使用される。設定要求生成部 812 は、以上の設定

要求Drrを通信部813に渡す。通信部813は、受け取った設定要求Drrを、伝送路91を通じて、利用権管理装置71に送信する(ステップS404)。

【0266】利用権管理装置71(図55参照)において、通信部715は、伝送路91を通じて送信されてくる設定要求Drrを受信して、ユーザ認証部716に渡す。ユーザ認証部716は、設定要求Drrにユーザ認証処理を行う(ステップS405)。より具体的には、ユーザ認証部716は、上述のユーザ情報DB713(図71(a)参照)を管理しており、受け取った設定要求Drrに設定されているメディア識別子lmdに一致するものが、当該ユーザ情報DB713に登録されているか否かを確認する。ユーザ認証部716は、ユーザ情報DB713に一致するものが登録されている場合に限り、今回設定要求Drrが、契約者βからのものであると判断する。さらに、このような判断結果に従って、ユーザ認証部716は、ユーザ情報DB713から、今回のメディア識別子lmdに対応するユーザ識別子lusrを取り出して、受け取った設定要求Drrと共に利用権管理部717に渡す。

【0267】利用権管理部717(図55参照)は、利用権データベース(以下、利用権DBと称する)714を管理している。また、利用権管理部717は、そこに設定されている設定要求識別子lrrに基づいて、ユーザ認証部716から設定要求Drrを渡されたことを認識する。このような認識結果に従って、利用権管理部717は、利用権DB714への利用権登録処理を行う(ステップS406)。より具体的には、利用権管理部717は、設定要求Drrから、コンテンツ識別子lcntおよび利用条件Ccntを取り出して、それらと、受け取ったユーザ識別子lusrとの組み合わせを利用権DB714に登録する。ここで、利用権管理部717は、設定要求Drrに設定されている利用条件Ccntで、契約者βが取得対象コンテンツデータDcntを利用する権利の設定を要求しているとみなす。つまり、利用権管理部717からみれば、利用条件Ccntは、取得対象コンテンツデータDcntを契約者βが利用できる権利を示す。以上の観点から、利用権管理部717は、設定要求Drrから取り出した利用条件Ccntを利用権情報Dratとして扱う。つまり、利用権DB714は、図71(b)に示すように、ユーザ識別子lusr、コンテンツ識別子lcntおよび利用権情報Dratの組み合わせの集まりとなる。これによって、利用権管理部717は、契約者βの取得対象コンテンツデータDcntの利用権を管理する。利用権管理部717は、以上の利用条件登録処理が終了すると、今回受け取った設定要求Drrをコンテンツ管理部718に渡す。

【0268】ここで、以上の利用権DB714に登録される利用権情報Dratの具体例について登録する。既に説明している通り、本実施形態では、利用条件Ccntは

利用回数であると仮定されている。さらに、今回の設定要求Drrには、メディア識別子lmdとして「x1」、コンテンツ識別子lcntとして「a」および利用条件Ccntとして「再生m回」(mは自然数)が設定されていると仮定する。以上の仮定下では、ユーザ認証部716は、ステップS405のユーザ認証処理において、ユーザ識別子lusrとしての「y1」を、ユーザ情報DB713から取り出して、利用権管理部717に渡す。従って、ステップS406では、図71(b)に示すように、1つの利用条件情報Dcntには、ユーザ識別子lusrとしての「y1」、コンテンツ識別子lcntとしての「a」および利用権情報Dratとしての「再生m回」が設定される。

【0269】なお、本ライセンス情報管理システムSc1の技術的特徴とは関係ないが、ステップS406において、利用権管理部717は、利用条件情報Dcntの登録毎に、ユーザ識別子lusrが割り当てられている契約者βに対して課金を行ってもよい。

【0270】コンテンツ管理部718は、設定要求Drrを受け取ると、図61のステップS204と同様の読み出し処理を行う(ステップS407)。その後、コンテンツ暗号化部719は、ステップS205と同様の暗号処理を行う(ステップS408)。さらに、送信データ生成部720は、ステップS206と同様の送信データ生成処理を行う(ステップS409)。その結果、ステップS206と同様に、送信データDtm(図62(b)参照)が、伝送路91を介して、機器201へと送信される(ステップS4010)。

【0271】機器201(図70参照)において、通信部813は、図61のステップS208と同様の受信処理を行う(図73:ステップS4011)。コンテンツ管理部814は、ステップS209と同様の蓄積処理を行う(ステップS4012)。その結果、コンテンツ蓄積部815には、図63を参照して説明したように、コンテンツ識別子lcntおよび暗号済みコンテンツデータDecntの組み合わせが、いくつか蓄積されることになる。

【0272】前述の実施形態での説明と同様に、機器201には暗号済みコンテンツデータDecntが配信される。そのため、機器201は、コンテンツデータDcntを利用する場合には、利用権管理装置71により提供される復号鍵Kdで、暗号済みコンテンツデータDecntを復号する必要がある。ここで、本ライセンス情報管理システムSc1では、復号鍵Kdを、契約者βが操作中の機器201に提供するために、後で詳説するライセンス情報Dlcが用いられる。以下、図75~図77を参照して、ライセンス情報Dlcの取得およびコンテンツデータDcntの復号時における機器201および利用権管理装置71の動作について説明する。

【0273】まず、契約者βは、機器201を操作し

て、コンテンツ蓄積部815にアクセスして、そこに蓄積されている暗号済みコンテンツデータDecntの中から、今回利用したいものを特定する。ここで、以下の説明において、今回指定された暗号済みコンテンツデータDecntを、復号対象コンテンツデータDecntと称する。

【0274】コンテンツ管理部814（図70参照）は、コンテンツ蓄積部815を管理しており、契約者βにより特定された復号対象コンテンツデータDecntに付加されているコンテンツ識別子Icntを、当該コンテンツ蓄積部815から取り出す。発行要求生成部816は、コンテンツ管理部814により取り出されたコンテンツ識別子Icntを受け取る（ステップS501）。

【0275】次に、発行要求生成部816は、識別子抽出部2022に、機器識別子I dvおよびメディア識別子I mdのいずれか一方を選択して、自身に返すように指示する。識別子抽出部2022は、発行要求生成部816の指示に応答して、可搬型記録媒体101が装着されている場合には、インターフェイス2021を通じて、当該可搬型記録媒体101に格納されているメディア識別子I mdを取り出す。発行要求生成部816は、識別子抽出部2022により取り出されたメディア識別子I mdを受け取る（ステップS502）。

【0276】ここで、識別子抽出部2022は、前述したように、機器201に可搬型記録媒体101が装着されていない場合、機器識別子格納部811から、機器識別子I dvを取り出して、設定要求生成部812に渡す。しかし、この場合、契約者αが、機器201を使って、ライセンス情報D lcの提供を受けることとなる。このような場合については、本変形例の目的とは関係なく、さらには、識別子抽出部2022が機器識別子I dvを取り出す場合における、機器201における動作については、前述の実施形態の説明から明らかであるため、その説明を省略する。

【0277】その後、発行要求生成部816は、メディア識別子I mdおよびコンテンツ識別子I cntに、発行要求識別子I irを付加して、発行要求Dir（図74（b）参照）を生成する（ステップS503）。ここで、発行要求Dirは、上述のライセンス情報D lcの提供を利用権管理装置71に要求するための情報である。また、発行要求識別子I irは、利用権管理装置71が発行要求Dirを特定するために使用される。発行要求生成部816は、以上の発行要求Dirを通信部813に渡す。通信部813は、受け取った発行要求Dirを伝送路91を通じて、利用権管理装置71に送信する（ステップS504）。

【0278】利用権管理装置71において、通信部715（図55参照）は、伝送路91を通じて送信されてくる発行要求Dirを受信して、ユーザ認証部716に渡す。ユーザ認証部716は、発行要求Dirを受け取ると、ユーザ認証部716は、発行要求Dirにユーザ認証

処理を行う（ステップS505）。より具体的には、ユーザ認証部716は、受け取った発行要求Dirに設定されているメディア識別子I mdに一致するものが、ユーザ情報DB713（図71（a）参照）に登録されているか否かを確認する。ユーザ認証部716は、ユーザ情報DB713に一致するものが登録されている場合に限り、今回の発行要求Dirが、契約者βからのものであると判断する。さらに、このような判断結果に従って、ユーザ認証部716は、ユーザ情報DB713から、今回のメディア識別子I mdに対応するユーザ識別子I usrを取り出して、受け取った発行要求Dirと共に利用権管理部717に渡す。

【0279】利用権管理部717は、発行要求Dirに設定されている発行要求識別子I irに基づいて、今回、ユーザ認証部716から発行要求Dirを渡されたことを認識する。このような認識結果に従って、利用権管理部717は、受け取った発行要求Dirからコンテンツ識別子I cntを取り出す（ステップS506）。次に、利用権管理部717は、受け取ったユーザ識別子I usrおよび取り出したコンテンツ識別子I cntの組み合わせが、利用権DB714（図71（b）参照）に登録されているか否かを判断する（ステップS507）。

【0280】利用権管理部717は、ステップS507で「Yes」と判断した場合、それらと同じ組みの利用権情報D ratを参照して、契約者βが操作中の機器201に利用許可を与えることができるか否かを判断する（ステップS508）。ステップS508で「Yes」と判断した場合、利用権管理部717は、利用権情報D ratの一部または全てを取り出す（ステップS509）。ここで、以下の説明において混同が生じることを避けるため、ステップS509において取り出された一部または全ての利用権情報D ratのことを、今回の発行要求Dirにより特定される契約者βの機器201にコンテンツデータD cntの利用を許可するための情報であるという観点から、利用許可情報D lwと称する。つまり、ステップS509では、利用許可情報D lwが生成される。

【0281】利用許可情報D lwの生成により、契約者βのために登録されている利用権情報D ratの一部または全てが使用される。そのため、ステップS509の次に、利用権管理部717は、ステップS509で一部または全部が取り出された利用権情報D ratを更新する（図75：ステップS5010）。

【0282】ここで、以上のステップS506～S5010の処理の具体例について登録する。今、利用権DB714には、図71（b）に示すように、ユーザ識別子I usrとしての「y1」、コンテンツ識別子I cntとしての「a」および利用権情報D ratとしての「再生m回」の組みが登録されていると仮定する。また、今回、機器201は、メディア識別子I mdとしての「x2」お

およびコンテンツ識別子 I_{cnt} としての「a」が設定されている発行要求 Dir を送信すると仮定する。

【0283】以上の仮定下では、ステップ $S506$ において、利用権管理部 717 は、ユーザ識別子 I_{usr} としての「y1」を受け取り、さらに、発行要求 Dir から、コンテンツ識別子 I_{cnt} としての「a」を取り出す。また、ステップ $S507$ において、ユーザ識別子 I_{usr} としての「y1」およびコンテンツ識別子 I_{cnt} としての「a」の組みが、利用権 $DB714$ に登録されていると判断される。このように判断されると、ステップ $S508$ において、同じ組みの利用権情報 D_{rqt} には、「再生 m 回」と設定されているので、契約者 β が操作中の機器 201 の利用許可を与えてもよいと判断される。このように判断されると、ステップ $S509$ において、利用許可情報 D_{lw} が生成される。この時生成される利用許可情報 D_{lw} としては、例えば、「再生 n 回」が挙げられる。ここで、 n は、上述の m を超えない自然数であり、より好ましくは、機器 201 の処理能力に応じて設定される。例えば、機器 201 が相対的に低い性能のハードウェアを搭載している場合であれば、 n は、「1」のように、機器 201 が復号対象コンテンツデータ $Decnt$ を利用可能な最低限の値に設定されることが好ましい。

【0284】以上のステップ $S506 \sim S509$ により、機器 201 に装着された可搬型記録媒体 101 (メディア識別子 I_{md} が「x2」) がコンテンツデータ D_{cnt} (コンテンツ識別子 I_{cnt} 「a」) を再生する権利を n 回使うことになる。そのため、ステップ $S5010$ において、契約者 β の利用権情報 D_{rqt} が「再生 m 回」から「再生 $(m-n)$ 回」に更新される。

【0285】以上のようにして生成した利用許可情報 D_{lw} を、利用権管理部 717 (図55参照) は、発行要求 Dir と一緒に、ライセンス情報生成部 721 に渡す。より具体的には、ライセンス情報生成部 721 は、図56に示すように、ハッシュ値生成部 7211 およびライセンス情報組立部 7212 を含んでいる。ハッシュ値生成部 7211 には、利用許可情報 D_{lw} のみが渡され、また、ライセンス情報組立部 7212 には、利用許可情報 D_{lw} および発行要求 Dir の双方が渡される。

【0286】まず、ハッシュ値生成部 7211 は、図64のステップ $S308$ と同様にして、ハッシュ値 V_{hs} を生成し (ステップ $S5011$)、生成したハッシュ値 V_{hs} をライセンス情報組立部 7212 に渡す。ライセンス情報組立部 7212 は、受け取った発行要求 Dir を復号鍵管理部 722 に渡す。復号鍵管理部 722 (図55参照) は、前述した復号鍵 $DB712$ (図59(b)参照) を管理する。復号鍵管理部 722 は、受け取った発行要求 Dir に設定されているコンテンツ識別子 I_{cnt} およびメディア識別子 I_{md} を取り出す。さらに、復号鍵管理部 722 は、コンテンツ識別子 I_{cnt} と同じ組みの復号鍵 K_d を復号鍵 $DB712$ から取り出して、メディア

識別子 I_{md} と一緒に復号鍵暗号化部 723 に渡す。復号鍵暗号化部 723 は、受け取った復号鍵 K_d を、同時に受け取ったメディア識別子 I_{md} で暗号化して (ステップ $S5012$)、暗号済みの復号鍵 K_{ed} を生成する。以上の暗号済み復号鍵 K_{ed} は、ライセンス情報組立部 7212 に渡される。

【0287】ライセンス情報組立部 7212 は、発行要求 Dir および利用許可情報 D_{lw} 、ハッシュ値 V_{hs} ならびに暗号済み復号鍵 K_{ed} のすべてが揃うと、図65のステップ $S3010$ と同様にして、図67(b)に示すライセンス情報 D_{lc} を生成する (ステップ $S5013$)。以上のライセンス情報 D_{lc} は、通信部 715 に渡される。通信部 715 から、伝送路 91 を通じて、機器 201 に送信される (ステップ $S5014$)。

【0288】機器 201 (図70参照) において、通信部 813 は、ステップ $S3012$ と同様にして、伝送路 91 を通じて送信されてくるライセンス情報 D_{lc} を受信し (ステップ $S5015$)、ライセンス情報処理部 817 に渡す。

【0289】ライセンス情報処理部 817 は、図58に示すように、改竄判定部 8171 と、ハッシュ値生成部 8172 と、利用許可判定部 8173 と、復号鍵復号部 8174 とを含んでいる。通信部 813 からのライセンス情報 D_{lc} は、まず、改竄判定部 8171 に渡される。改竄判定部 8171 は、まず、ステップ $S3013$ と同様に、受け取ったライセンス情報 D_{lc} から、利用許可情報 D_{lw} を取り出し、さらに、ハッシュ値 V_{hs} を外部ハッシュ値 V_{ehs} として取り出し (ステップ $S5016$)、取り出した利用許可情報 D_{lw} を、ハッシュ値生成部 8172 に渡し、外部ハッシュ値 V_{ehs} をそのまま保持する。

【0290】ハッシュ値生成部 8172 は、ステップ $S3014$ と同様にして、内部ハッシュ値 V_{lhs} を生成して (ステップ $S5017$)、改竄判定部 8171 に返す。

【0291】改竄判定部 8171 は、上述の内部ハッシュ値 V_{lhs} を受け取ると、ステップ $S3015$ と同様にして、利用許可情報 D_{lw} が改竄されているか否かを判定し (ステップ $S5018$)、「Yes」と判定した場合には、今回受け取ったライセンス情報 D_{lc} を利用許可判定部 8173 に渡す。

【0292】利用許可判定部 8173 は、受け取ったライセンス情報 D_{lc} を参照して、ステップ $S3016$ と同様にして、復号対象コンテンツデータ $Decnt$ の利用が許可されているか否かを判定する (ステップ $S5019$)。利用許可判定部 8173 は、ステップ $S5019$ において「Yes」と判断した場合に限り、受け取ったライセンス情報 D_{lc} から、暗号済み復号鍵 K_{ed} を取り出して、復号鍵復号部 8174 に渡す。

【0293】ここで、以上のステップ $S5019$ の処理

の具体例について説明する。前述の仮定に従えば、今回のライセンス情報D1cの利用許可情報D1wにより、コンテンツデータDcntの再生がn回だけ許可されている。かかる場合、利用許可判定部8173は、ステップS5019において、利用許可情報D1wに設定される再生回数が1以上であれば、復号対象コンテンツデータDecntの利用が許可されていると判断して、受け取ったライセンス情報D1cから暗号済み復号鍵Kedを取り出して、復号鍵復号部8174に渡す。

【0294】さて、復号鍵復号部8174は、利用許可判定部8173から暗号済み復号鍵Kedを受け取る。さらに、復号鍵復号部8174は、識別子抽出部2022に、機器識別子I dvおよびメディア識別子I mdのいずれか一方を選択して、自身に返すように指示する。識別子抽出部2022は、復号鍵復号部8174の指示にตอบสนองして、可搬型記録媒体101が装着されている場合には、インターフェイス2021を通じて、当該可搬型記録媒体101に格納されているメディア識別子I mdを取り出す。復号鍵復号部8174は、識別子抽出部2022により取り出されたメディア識別子I mdを受け取る。【0295】ここで、識別子抽出部2022は、機器201に可搬型記録媒体101が装着されていない場合、機器識別子格納部811から、機器識別子I dvを取り出して、復号鍵復号部8174に渡すことになる。このような場合については、本変形例の目的とは関係なく、さらには、識別子抽出部2022が機器識別子I dvを取り出す場合における、機器201における動作については、前述の実施形態と同様であるため、その説明を省略する。

【0296】以上のようにして、メディア識別子I mdを受け取ると、復号鍵復号部8174は、暗号済み復号鍵Kedを、メディア識別子I mdで復号して(図77:ステップS5020)、復号鍵Kdをコンテンツ復号部818に渡す。

【0297】ところで、コンテンツ管理部814は、ステップS501において、コンテンツ識別子I cntだけでなく、前述の復号対象コンテンツデータDecntを取り出す。取り出された復号対象コンテンツデータDecntは、コンテンツ復号部818に渡される。コンテンツ復号部818は、復号鍵復号部8174から受け取った復号鍵Kdで、復号対象コンテンツデータDecntを復号して(ステップS5021)、コンテンツデータDcntをコンテンツ再生部819に渡す。コンテンツ再生部819は、受け取ったコンテンツデータDcntを再生して、音声出力する(ステップS5022)。これにより、契約者βは、事業者αから購入したコンテンツデータDcntが表す音楽を聴くことができる。以上説明したように、本ライセンス情報管理システムSc1によれば、契約者βは、自分が得た利用権情報D rqtを使って、別の契約者γが管理する機器201で、コンテンツデータD cnt

tを利用することが可能となる。これによって、より使い勝手のよいライセンス情報管理システムSc1を提供することが可能となる。

【0298】ここで、図76のステップS5018において、改竄判定部8171は、利用許可情報D1wが改竄されていると判定する場合がある。また、ステップS5019において、利用許可判定部8173は、復号対象コンテンツデータDecntの利用が許可されていないと判定する場合もある。このような場合、改竄判定部8171および利用許可判定部8173は、図66のステップS3020を実行して、今回受け取ったライセンス情報D1cを破棄する。

【0299】また、図75のステップS507において、利用権管理部717は、ユーザ識別子I usr およびコンテンツ識別子I cntの組み合わせが、利用権DB714(図71(b)参照)に登録されていないと判断する場合がある。さらに、ステップS508において、利用権管理部717は、契約者βが操作中の機器201に利用許可を与えないと判断する場合もある。このような場合、利用権管理部717は、図66のステップS3021を実行して、利用拒否情報D rjを生成して、通信部715に渡す。通信部715は、受け取った利用拒否情報D rjを、伝送路91を介して、機器201に送信する。これによって、前述の実施形態と同様に、機器201が、復号対象コンテンツデータDecntを復号しないようにすることができる。

【0300】なお、ステップS507において、利用権管理部717は、ユーザ識別子I usr およびコンテンツ識別子I cntの組み合わせが、利用権DB714(図71(b)参照)に登録されていないと判断する場合に、ユーザ識別子I usr、コンテンツ識別子I cnt および利用権情報D rqtを生成して、利用権DB714に登録するようにしてもよい。

【0301】なお、以上の変形例において、契約者β側には、前述の実施形態で説明した機器81が設置されるとして説明したが、これに限らず、上述の機器201が設置されてもよい。

【0302】また、以上の変形例において、機器201は、機器識別子格納部811を備えるとして説明した。しかしながら、契約者γ自身が機器201を使ってコンテンツデータD cnt およびライセンス情報D1cの提供を利用権管理装置71から受けない場合には、機器201は、機器識別子格納部811を備える必要性はない。

【0303】また、以上の変形例においても、前述の実施形態と同様に、互いに異なる利用権管理装置が図72および図73の処理と図75～図77の処理とを行うようにしてもよい。さらに、本変形例においても、最初にライセンス情報D1cの取得が行われ、その後、コンテンツデータD cntの取得が行われても良い。また、コンテンツデータD cntの取得およびライセンス情報D1cの

取得が同時並行して行われてもよい。

【0304】また、以上の変形例では、説明の便宜上、ユーザ情報DB713には、ユーザ識別子1usrと、機器識別子1dvおよび／またはメディア識別子1mdが登録されるとして説明した。しかしながら、前述の実施形態と同様に、ユーザ情報DB713にはさらに、契約者βを一意に特定可能な他のユーザ情報（例えば、住所および電話番号）が登録されてもよい。

【0305】また、以上の変形例は、前述の実施形態と同様、機器201におけるコンテンツ再生部819は、コンテンツデータDcntの種類に応じて、テレビ番組、映画、書籍および印刷物およびゲーム内容を映像出力可能なもの、ラジオ番組を音声出力可能なものに置換されてもよい。さらに、機器201は、以上のようなコンテンツ再生部819に代えて、復号されたコンテンツデータDcntを、外部の機器（テレビジョン受像機、ラジオ受信機、音楽再生機、電子ブックリーダー、ゲーム機器、PC、情報携帯端末、携帯電話、外部記憶装置等）に転送可能なインターフェイスを備えていてもよい。

【0306】また、以上の変形例においても、前述の実施形態と同様、SSL等の保護技術を適用するという条件で、ライセンス情報D1cは、暗号化されていない復号鍵Kdをそのまま含んでもよい。また、デジタルライツを保護するために、機器201には、可搬型記録媒体101に格納されるメディア識別子1mdでライセンス情報D1cを暗号化するアルゴリズムが組み込まれることがより好ましい。

【0307】また、以上の第6の変形例に係るインターフェイス2021および識別子抽出部2022は、第2の実施形態に係る機器51に組み込まれてもよい。このように、機器51aまたは51bに、インターフェイス2021および識別子抽出部2022の両者を組み込んだ場合、識別子抽出部2022は、ユーザの指定に従って、機器51aまたは51bの機器識別子格納部211に設定されている機器識別子1dvaまたは1dvbもしくは、可搬型記録媒体101に格納されているメディア識別子1mdのいずれかを使って、設定要求Drrを生成して、利用権管理装置41に送信する。これによって、ユーザは、機器51aまたは51bもしくは可搬型記録媒体101のいずれかを使って、コンテンツデータDcntを利用できるようになるので、より使い勝手の良いライセンス情報管理システムSbを実現できるようになる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る利用権管理装置11を収容したライセンス情報管理システムSaの全体構成を示すブロック図である。

【図2】図1の利用権管理装置11の詳細な構成を示すブロック図である。

【図3】図2のライセンス情報生成部121の詳細な構成を示すブロック図である。

【図4】図1の機器21aおよび21bの詳細な構成を示すブロック図である。

【図5】図4のライセンス情報処理部217の詳細な構成を示すブロック図である。

【図6】図2のコンテンツDB111および図2の復号鍵DB112を示す模式図である。

【図7】図2のユーザ情報DB113および図2の利用権DB114を示す模式図である。

【図8】コンテンツデータDcntの利用権設定および取得時における、機器21aおよび利用権管理装置11の動作を示すフローチャートである。

【図9】図8に示す処理の過程で送受される設定要求Drrおよび送信データDtrnのフォーマットを示す模式図である。

【図10】図4のコンテンツ蓄積部215に蓄積されるデータを示す模式図である。

【図11】ライセンス情報D1caの取得およびコンテンツデータDcntの復号時における機器21aおよび利用権管理装置11の動作を示す第1のフローチャートである。

【図12】ライセンス情報D1caの取得およびコンテンツデータDcntの復号時における機器21aおよび利用権管理装置11の動作を示す第2のフローチャートである。

【図13】ライセンス情報D1caの取得およびコンテンツデータDcntの復号時における機器21aおよび利用権管理装置11の動作を示す第3のフローチャートである。

【図14】図12～図13の処理の過程で送受される発行要求Dir、ライセンス情報D1cおよび利用拒否情報Drjのフォーマットを示す模式図である。

【図15】図1の利用権管理装置11の第1の変形例に係る利用権管理装置11aを収容したライセンス情報管理システムSa1の全体構成を示すブロック図である。

【図16】図15に示す利用権管理装置11aの詳細な構成を示すブロック図である。

【図17】図15に示す機器21cの詳細な構成を示すブロック図である。

【図18】図15の機器21cをユーザ情報DB113に登録するまでの機器21cおよび利用権管理装置11aの動作を示すフローチャートである。

【図19】図18の処理の過程で送受される登録要求Drc、登録完了通知Dscおよび登録拒否通知Dsrのフォーマットを示す模式図である。

【図20】図18の処理により更新されたユーザ情報DB113を示す模式図である。

【図21】図1の利用権管理装置11の第2の変形例に係る利用権管理装置11bの詳細な構成を示すブロック図である。

50 【図22】第2の変形例に係る機器21aまたは21b

の詳細な構成を示すブロック図である。

【図23】第2の変型例に係る機器21cの詳細な構成を示すブロック図である。

【図24】機器21cの機器識別子ldvcをユーザ情報DB113に登録する際における機器21aおよび利用権管理装置11bの動作を示すフローチャートである。

【図25】機器21cの機器識別子ldvcをユーザ情報DB113に登録する際における機器21cおよび利用権管理装置11bの動作を示すフローチャートである。

【図26】図24の処理の過程で送受される仮登録要求Dprscおよび仮登録完了通知Dpsccのフォーマットを示す模式図である。

【図27】図24および図25の処理により更新されたユーザ情報DB113を示す模式図である。

【図28】図25の処理の過程で送受される本登録要求Dcrscおよび本登録完了通知Dcscのフォーマットを示す模式図である。

【図29】図1の利用権管理装置11の第3の変型例に係る利用権管理装置11cの詳細な構成を示すブロック図である。

【図30】第3の変型例に係る機器21aまたは21bの詳細な構成を示すブロック図である。

【図31】第3の変型例に係る機器21cの詳細な構成を示すブロック図である。

【図32】機器21cの機器識別子ldvcをユーザ情報DB113に登録する際における、機器21cおよび利用権管理装置11cの動作を示すフローチャートである。

【図33】機器21cの機器識別子ldvcをユーザ情報DB113に登録する際における、機器21aおよび利用権管理装置11cの動作を示すフローチャートである。

【図34】図32の処理の過程で送受されるパスワード要求Dtpsおよびパスワード通知Dpsのフォーマットを示す模式図である。

【図35】図32および図33の処理により更新されたユーザ情報DB113を示す模式図である。

【図36】図33の処理の過程で送受される登録要求Drscおよび登録完了通知Dscのフォーマットを示す模式図である。

【図37】図1の利用権管理装置11の第4の変型例に係る利用権管理装置11dの詳細な構成を示すブロック図である。

【図38】第4の変型例に係る機器21aまたは21bの詳細な構成を示すブロック図である。

【図39】第4の変型例に係る機器21cの詳細な構成を示すブロック図である。

【図40】機器21cの機器識別子ldvcをユーザ情報DB113に登録するまでの機器21a、機器21cおよび利用権管理装置11dの動作を示すフローチャート

である。

【図41】図40の処理の過程で送受される第1の登録要求Drsc1、第2の登録要求Drscおよび登録完了通知Dscのフォーマットを示す図である。

【図42】図1の利用権管理装置11の第5の変型例に係る利用権管理装置11eを収容したライセンス情報管理システムSa5の全体構成を示すブロック図である。

【図43】図42に示す利用権管理装置11eの詳細な構成を示すブロック図である。

【図44】図42に示す機器21bの詳細な構成を示すブロック図である。

【図45】機器21bの機器識別子ldvbをユーザ情報DB113および利用権DB114から削除するまでの機器21bおよび利用権管理装置11eの動作を示すフローチャートである。

【図46】図45の処理の過程で送受される削除要求Dnwbおよび削除完了通知Dswbのフォーマットを示す模式図である。

【図47】図45の処理により更新されたユーザ情報DB113を示す模式図である。

【図48】本発明の第2の実施形態に係る利用権管理装置41を収容したライセンス情報管理システムSbの全体構成を示すブロック図である。

【図49】図48の利用権管理装置41の詳細な構成を示すブロック図である。

【図50】図48の機器51aおよび51bの詳細な構成を示すブロック図である。

【図51】コンテンツデータDcntの取得時における機器51aおよび利用権管理装置41の動作を示すフローチャートである。

【図52】図49の利用権DB114を示す模式図である。

【図53】図51の処理の過程で送受される第2の設定要求Drr2bのフォーマットを示す図である。

【図54】本発明の第3の実施形態に係るライセンス情報管理システムScの全体構成を示すブロック図である。

【図55】図54の利用権管理装置71の詳細な構成を示す機能ブロック図である。

【図56】図55のライセンス情報生成部721の詳細な構成を示す図である。

【図57】図54の機器81の詳細な構成を示す機能ブロック図である。

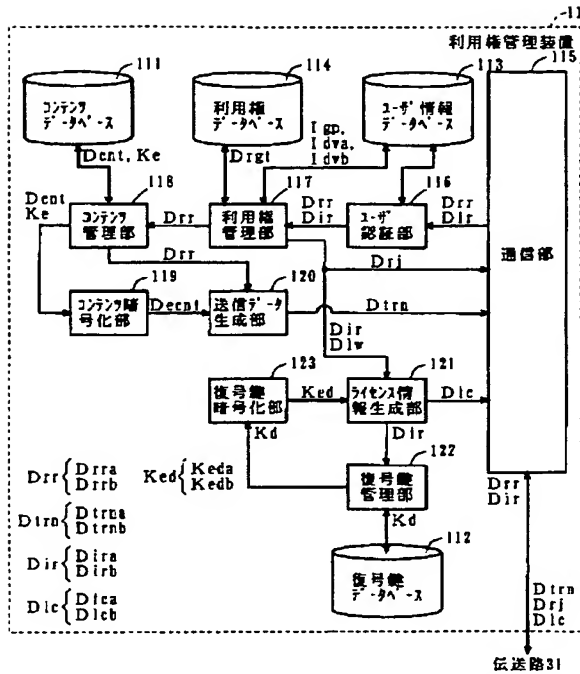
【図58】図57のライセンス情報処理部817の詳細な構成を示す機能ブロック図である。

【図59】図55のコンテンツDB711および図55の復号鍵DB712を示す模式図である。

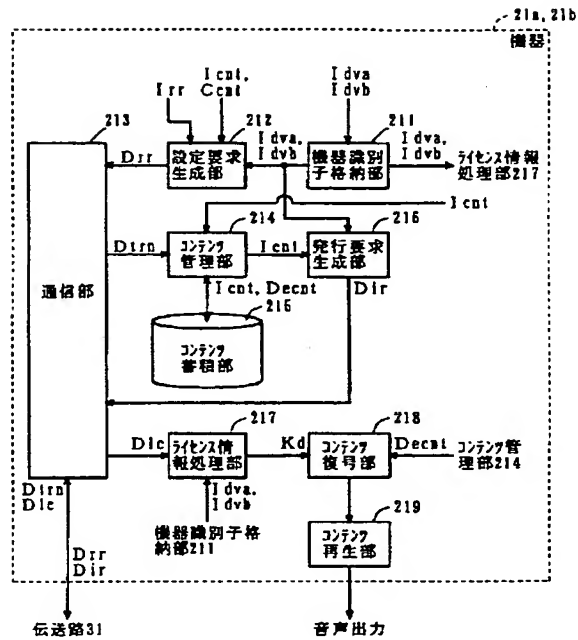
【図60】図55のユーザ情報DB713および利用権DB714を示す模式図である。

【図61】コンテンツデータDcntの取得時における機

【圖2】

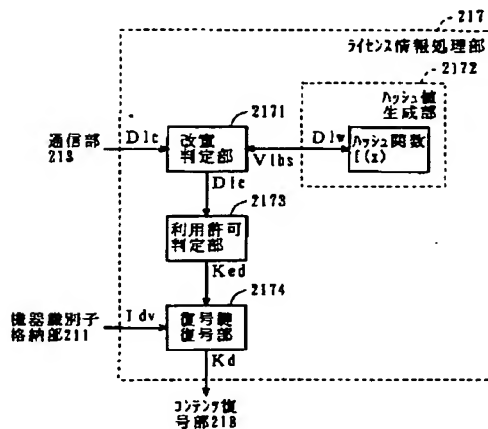


【图4】

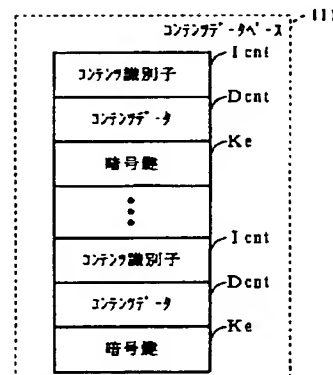


【図6】

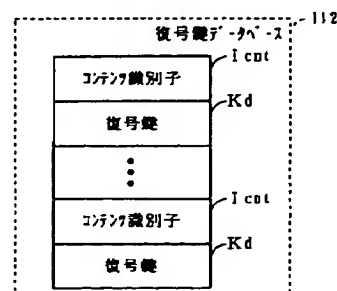
【圖 5】



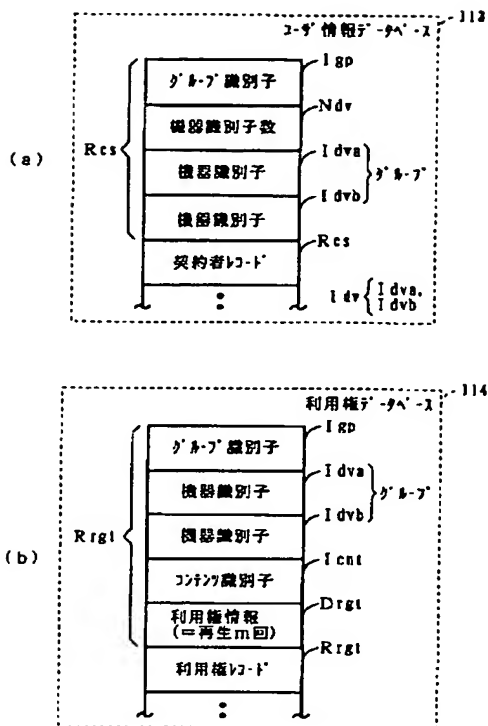
(a)



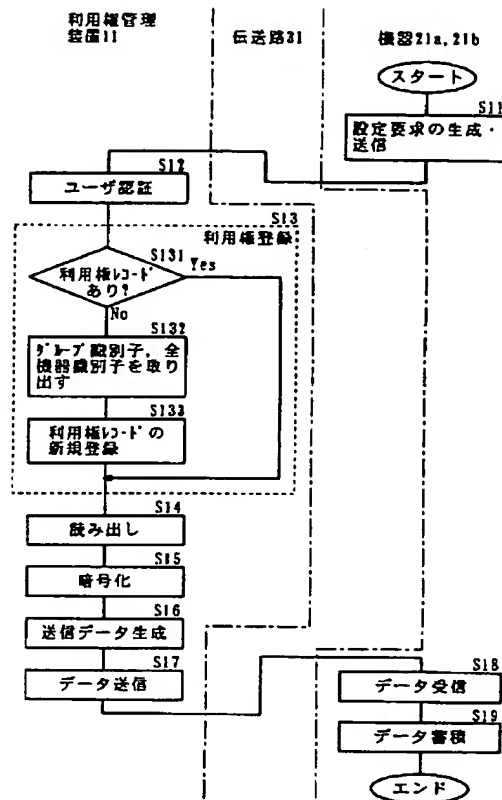
(b)



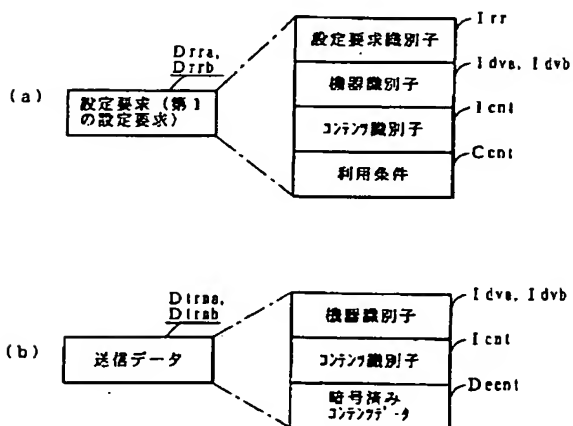
【図7】



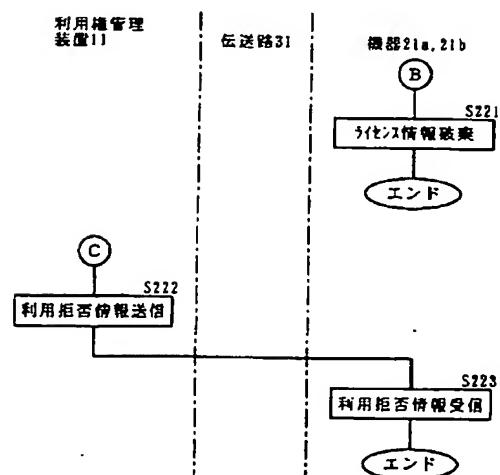
【図8】



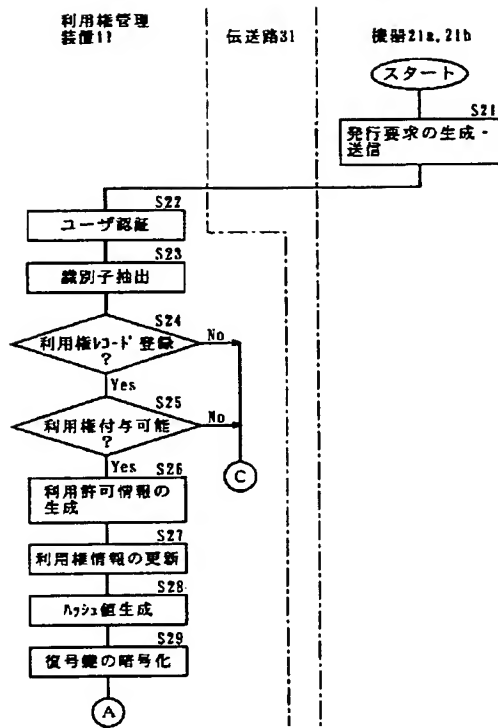
【図9】



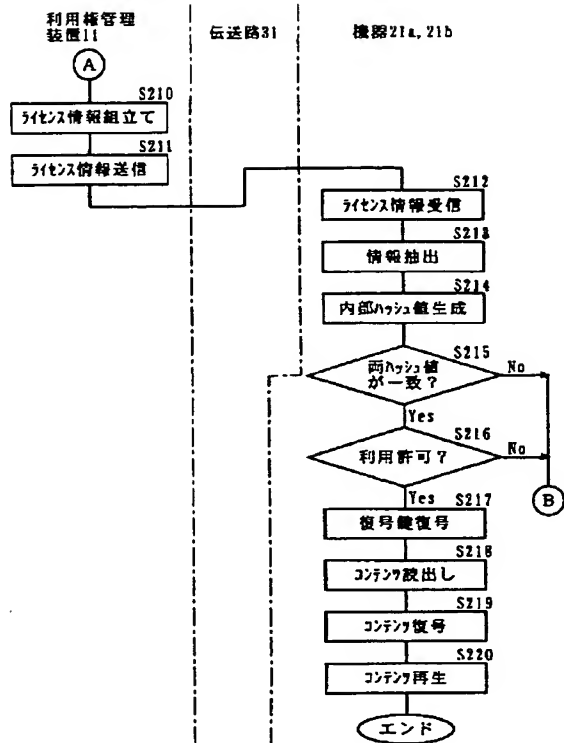
【図13】



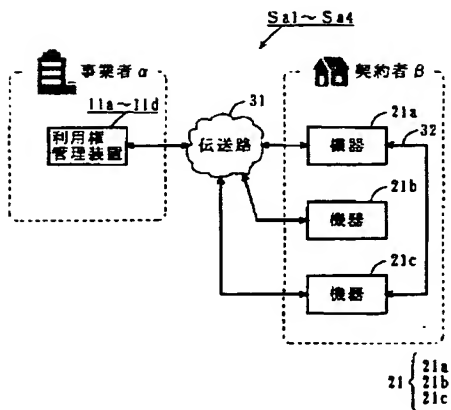
【図11】



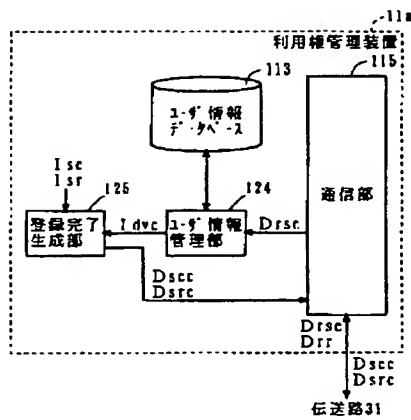
【図12】



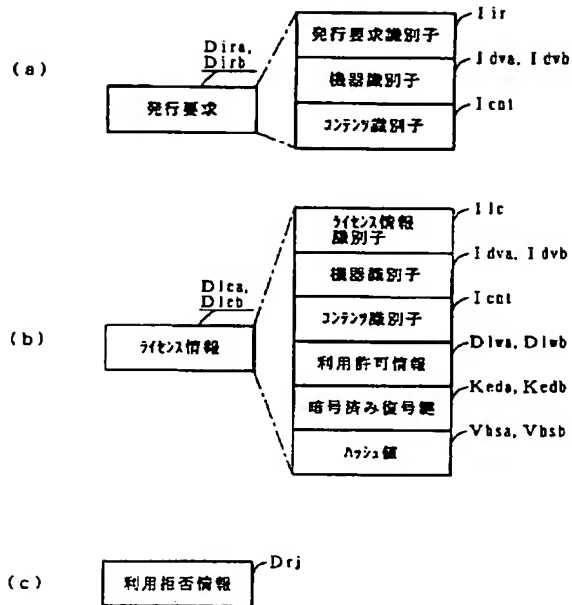
【図15】



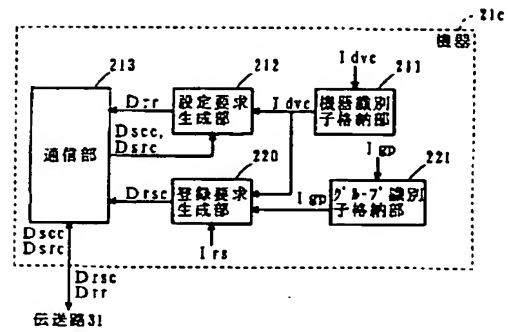
【図16】



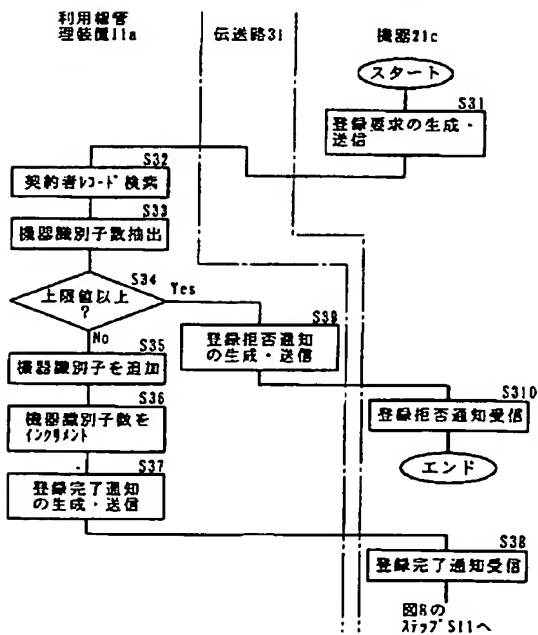
【図14】



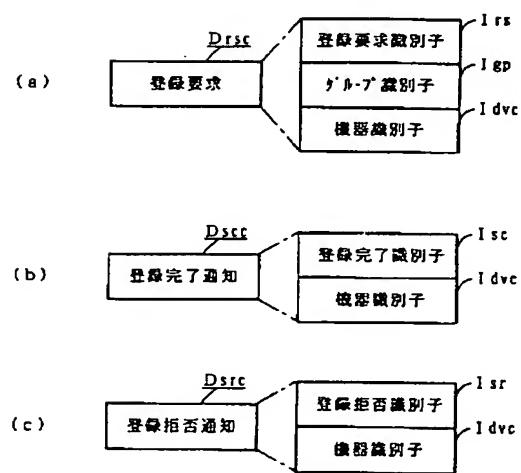
【図17】



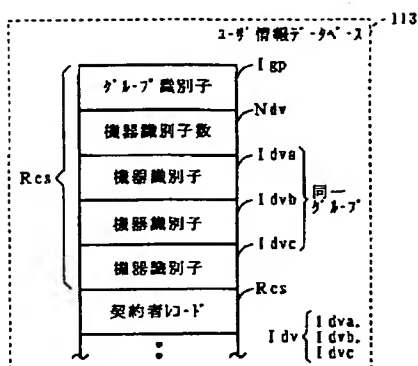
【図18】



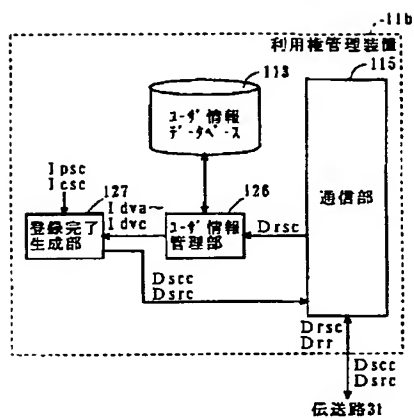
【図19】



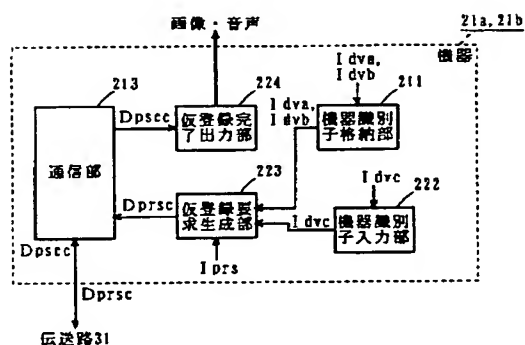
【圖20】



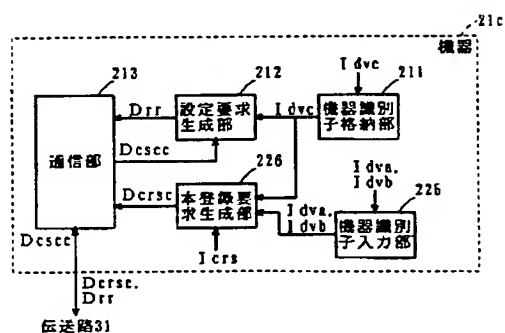
【圖 21】



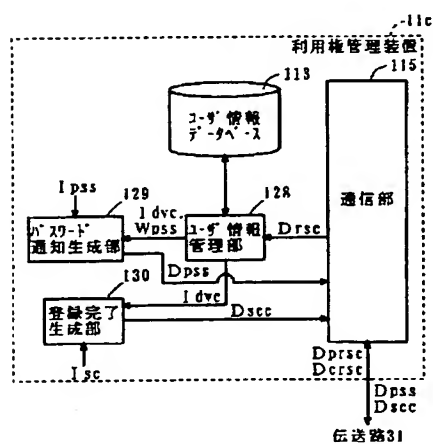
【圖 22】



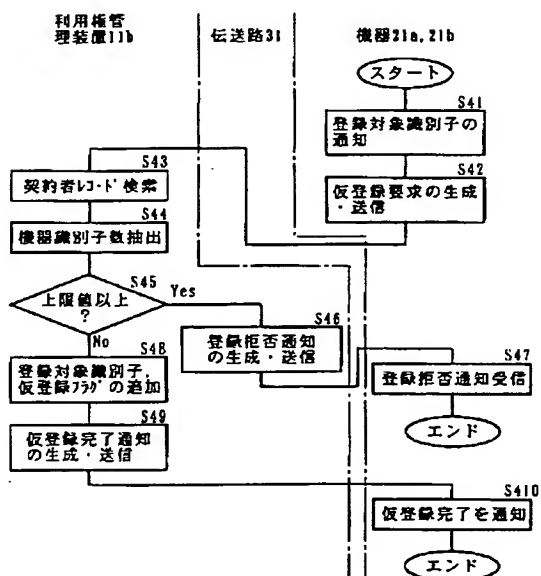
【圖 23】



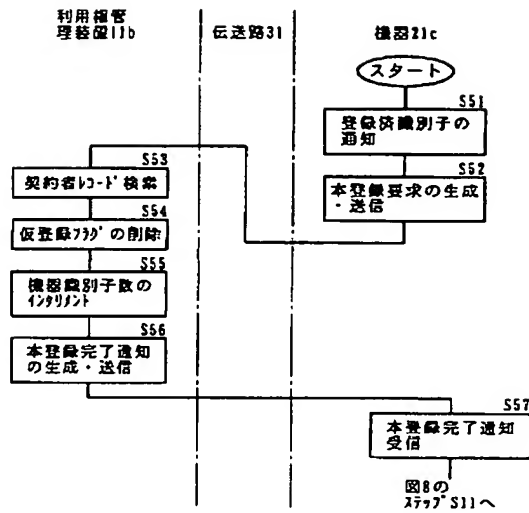
【圖29】



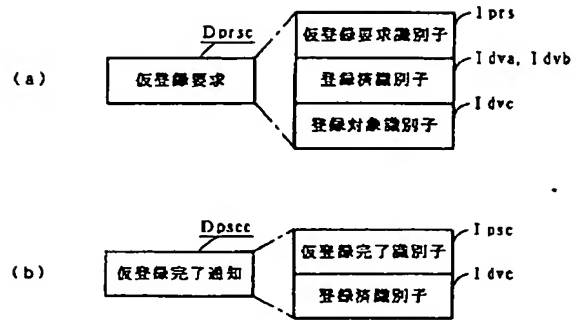
【圖24】



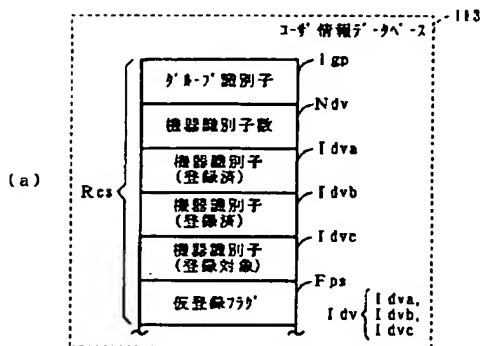
【図25】



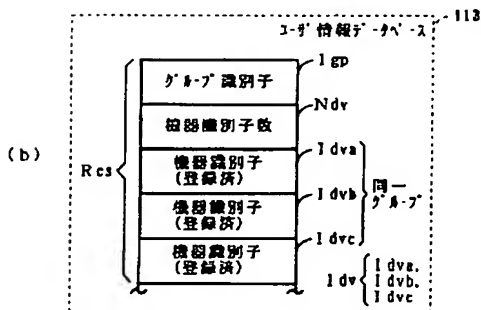
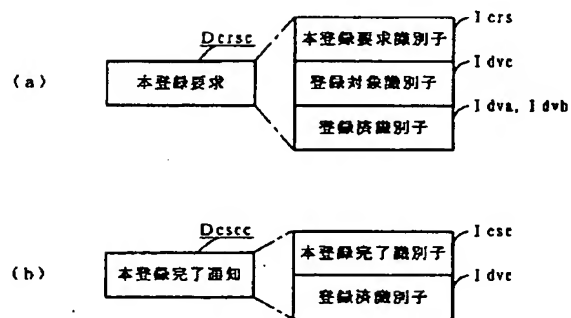
【図26】



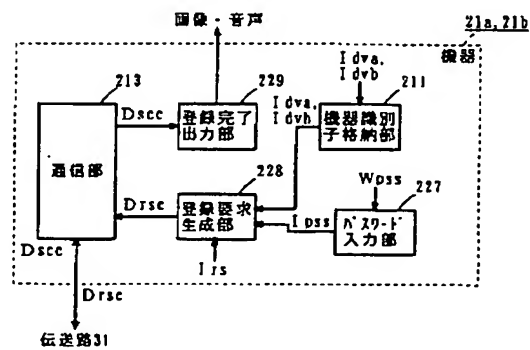
【図27】



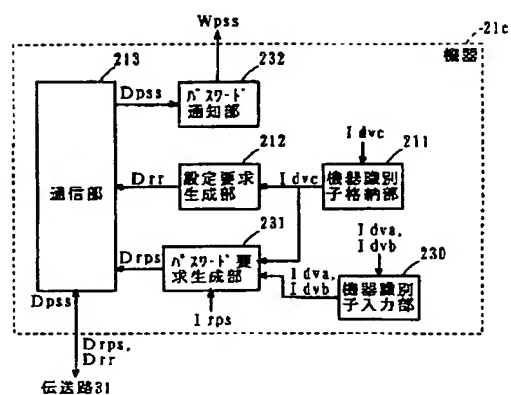
【図28】



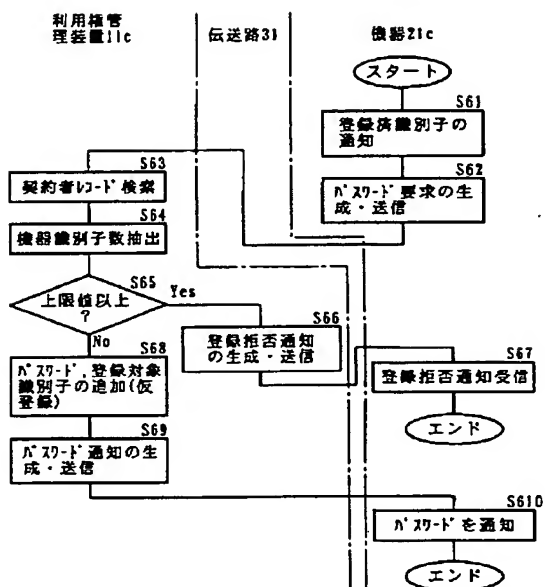
【図30】



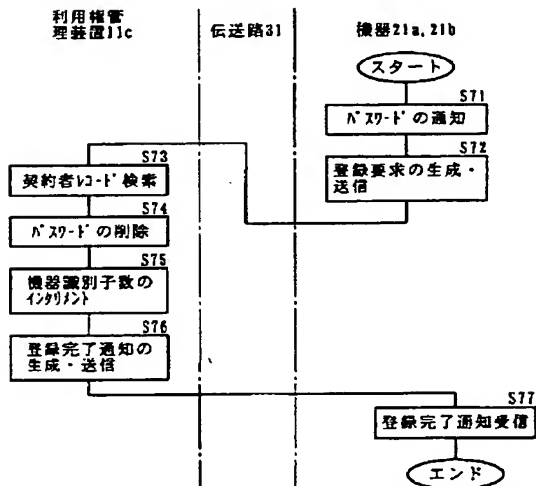
【圖 3 1】



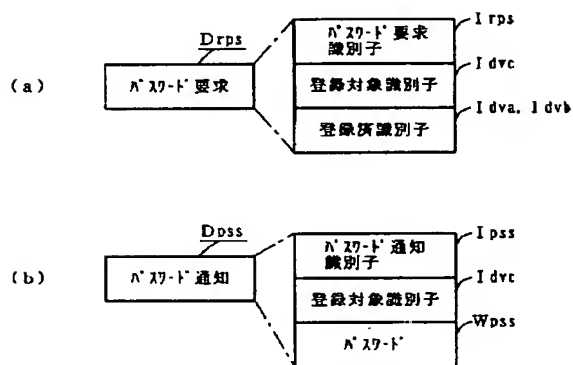
【圖 32】



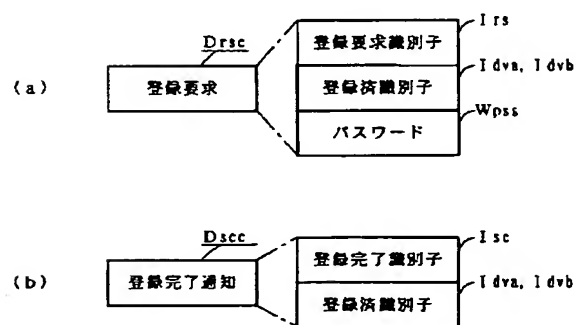
【圖 3 3】



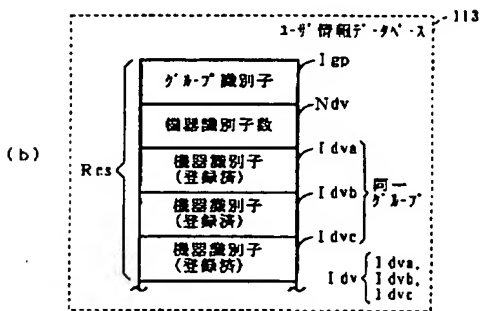
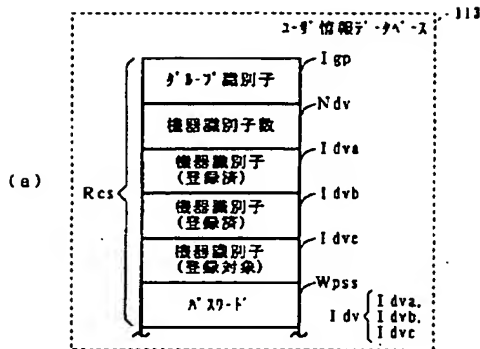
【圖 34】



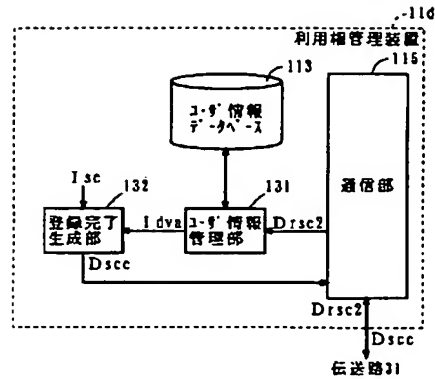
【圖 36】



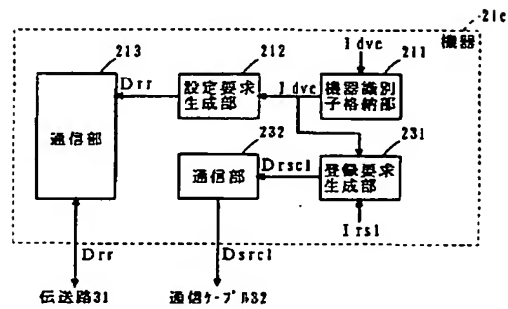
【図35】



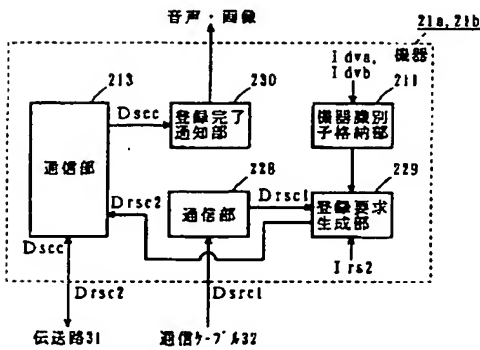
【図37】



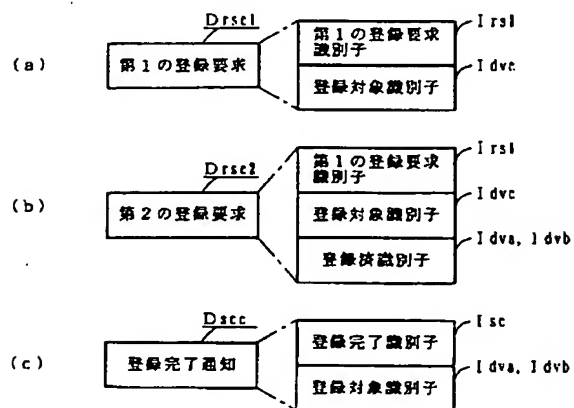
【図39】



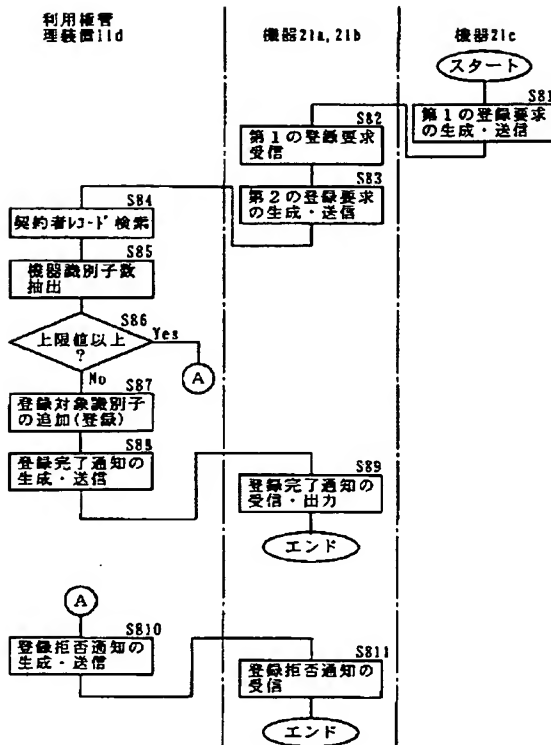
【図38】



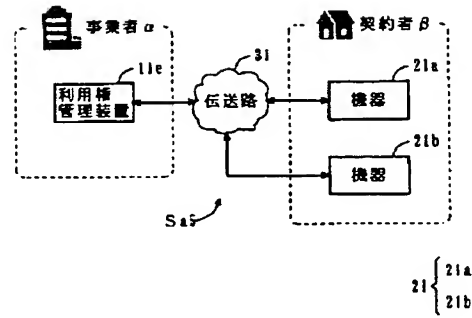
【図41】



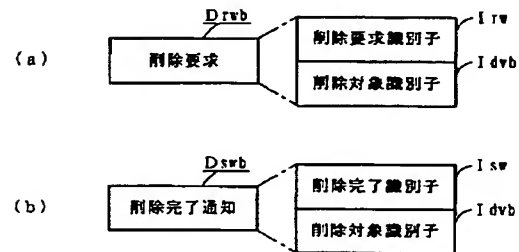
【図40】



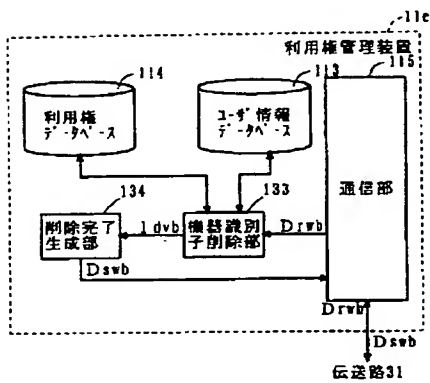
【図42】



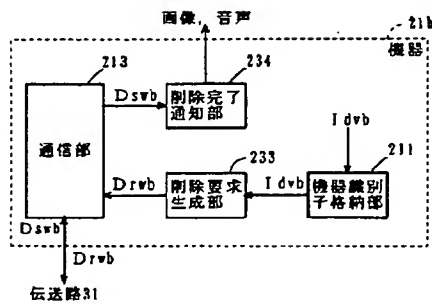
【図46】



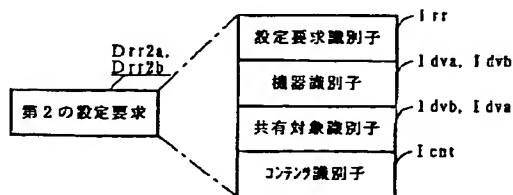
【図43】



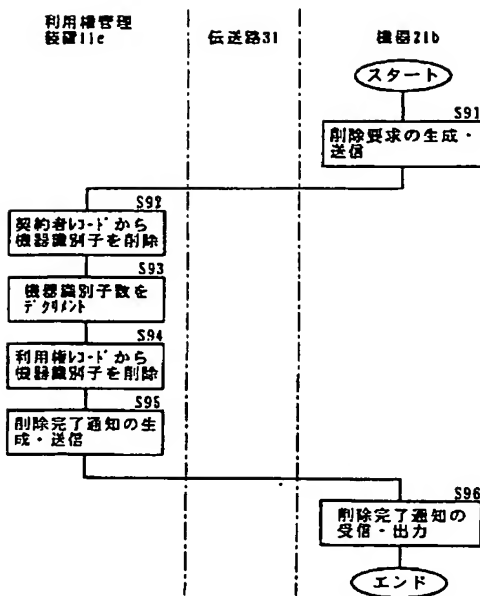
【図44】



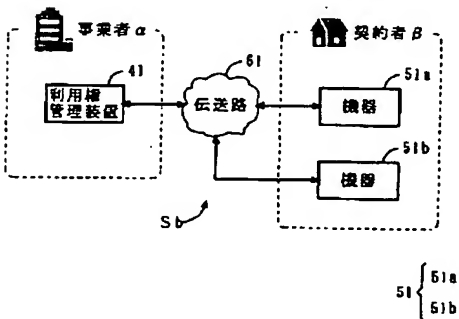
【図53】



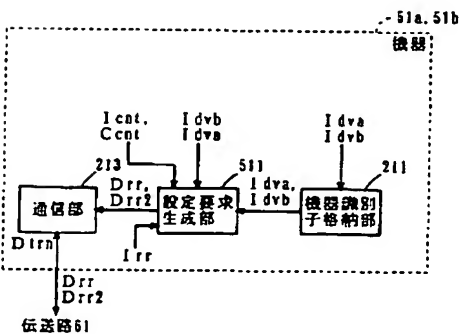
【圖 45】



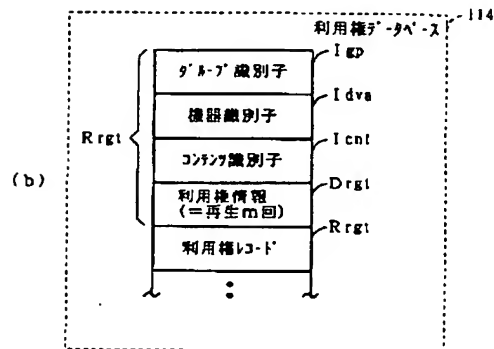
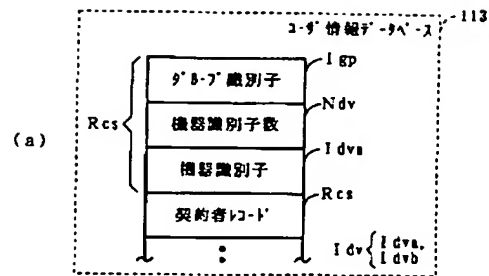
【例 48】



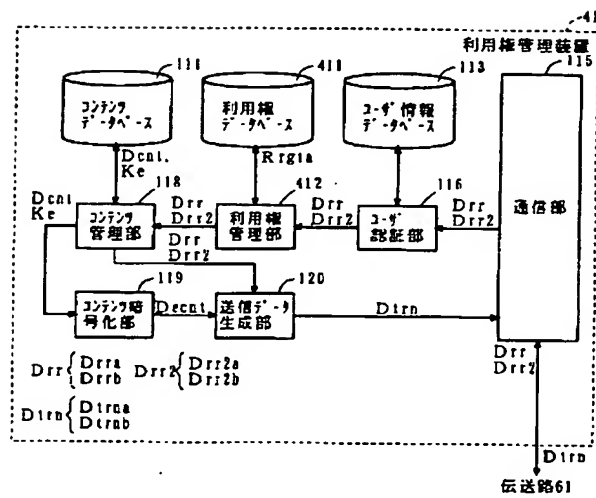
【圖 50】



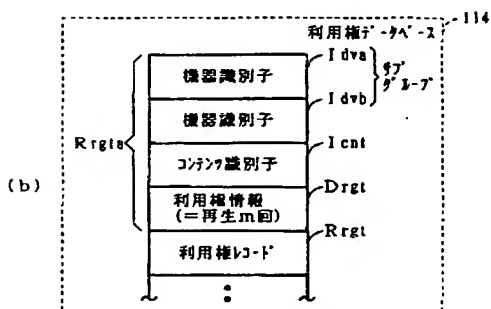
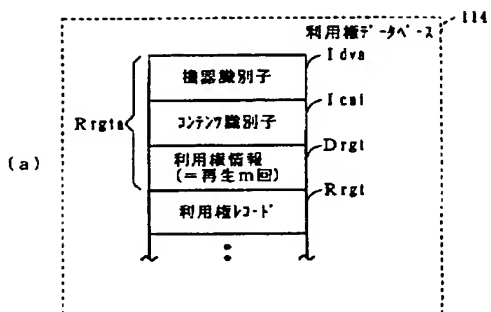
【圖 47】



【圖 49】

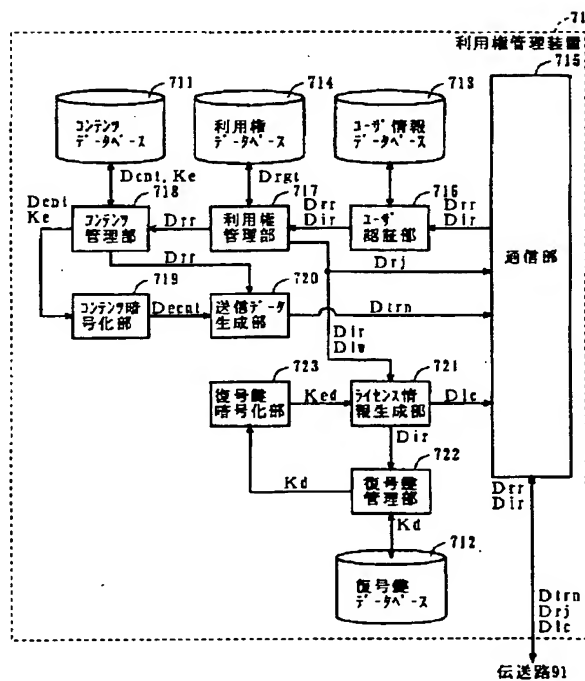


【图 5 2】

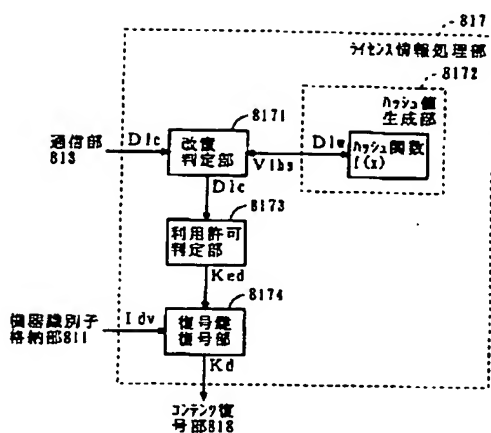


【圖 55】

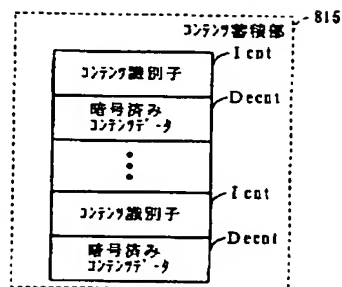
Figure 1 is a block diagram illustrating the connection between a user (利用者 α) and a partner (契約者 β). On the left, the user side is enclosed in a dashed box and contains a '利用権管理装置' (71) connected to a '伝送路' (91). On the right, the partner side is enclosed in a dashed box and contains a '機器' (81) connected to the same '伝送路' (91). A dashed line labeled 'S' connects the two sides.



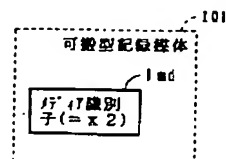
【圖 58】



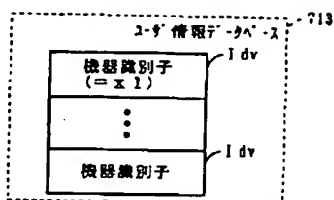
【图 6-3】



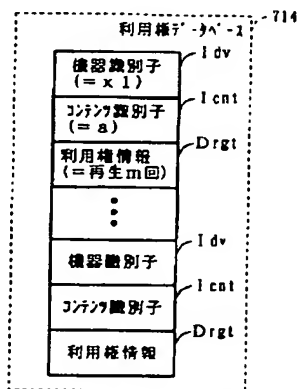
【圖 69】



【圖 60】

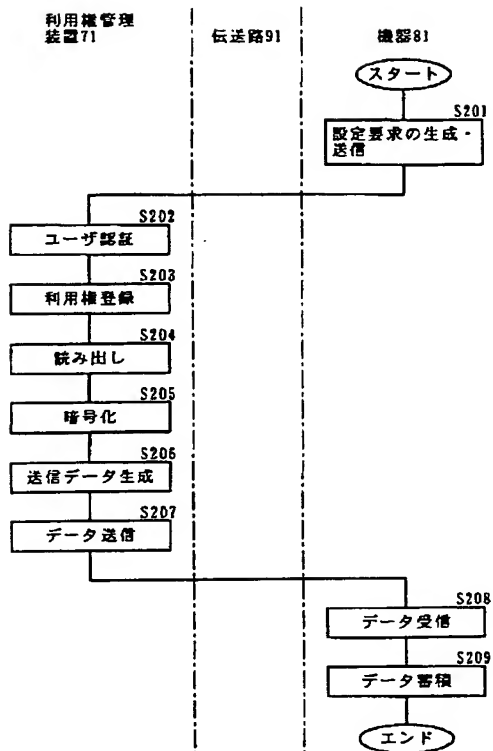


【圖 69】

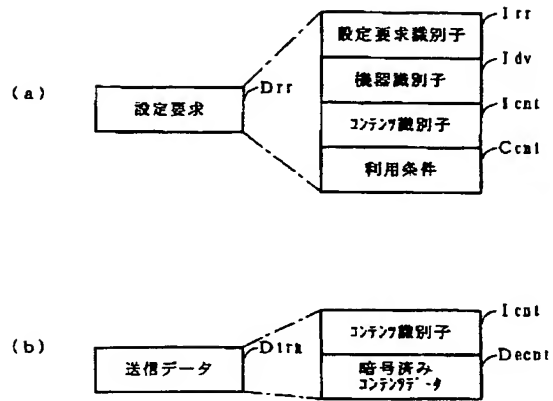


----- 101

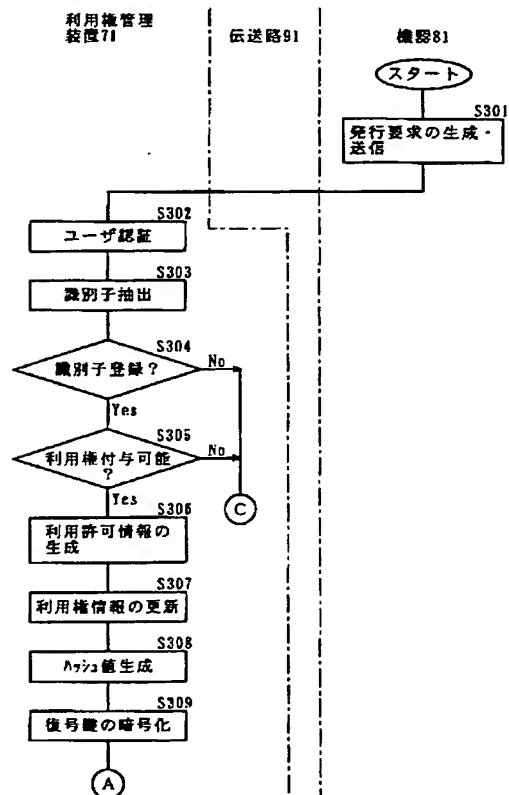
【図61】



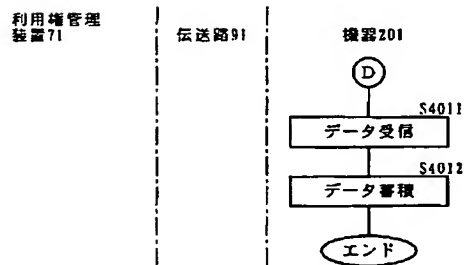
【図62】



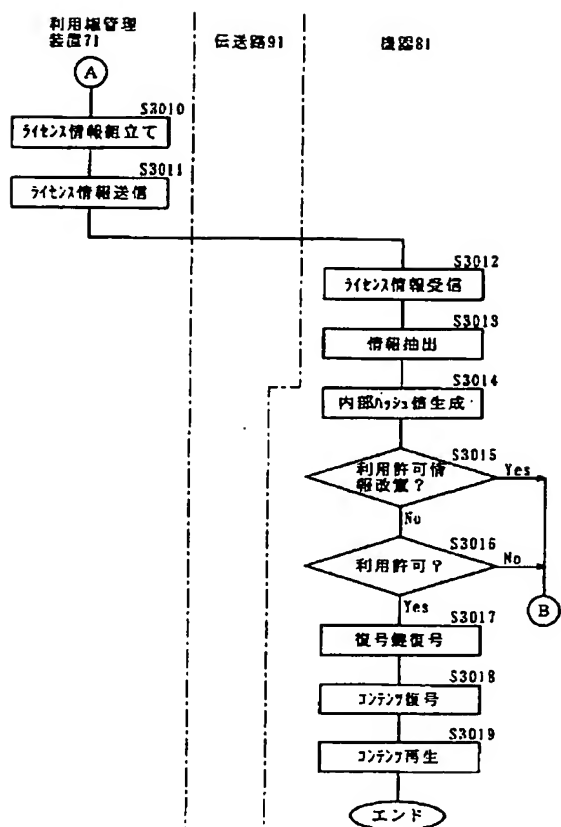
【図64】



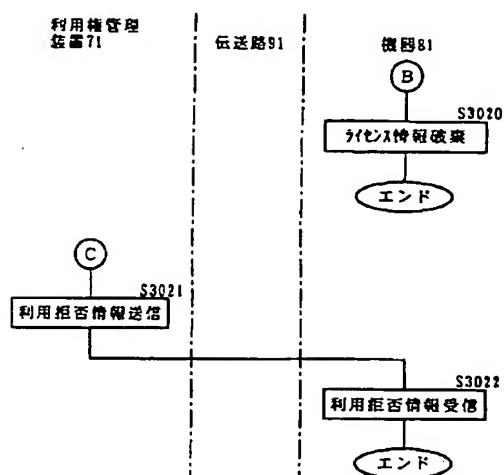
【図73】



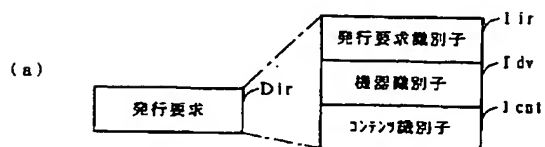
【図65】



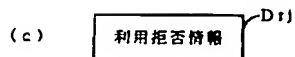
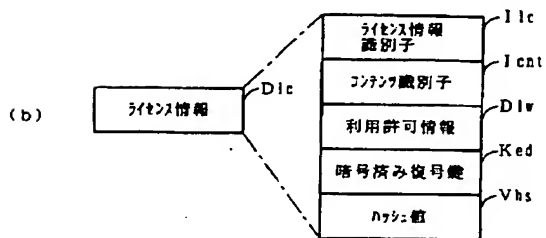
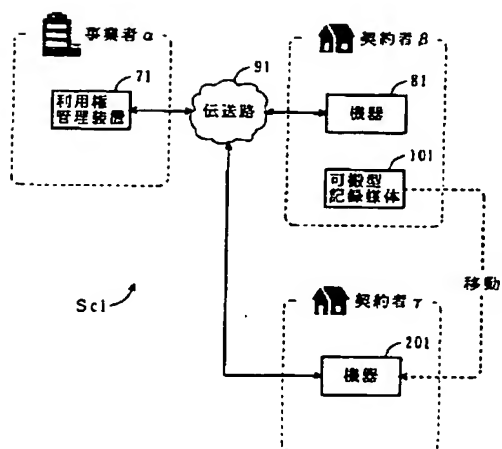
【図66】



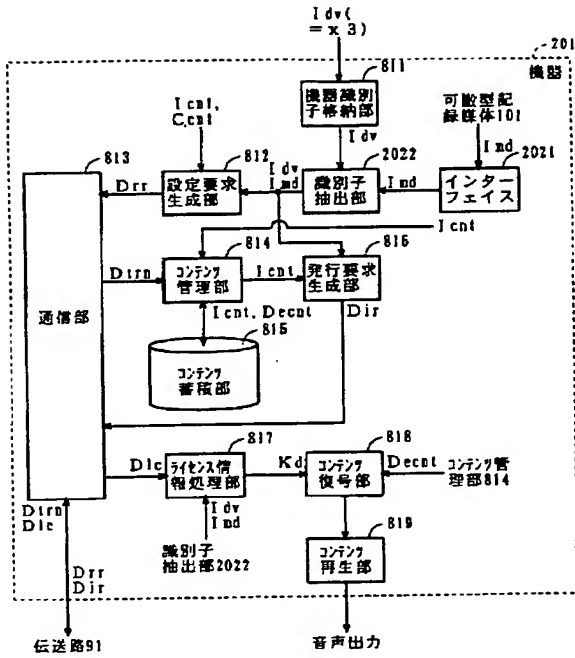
【図67】



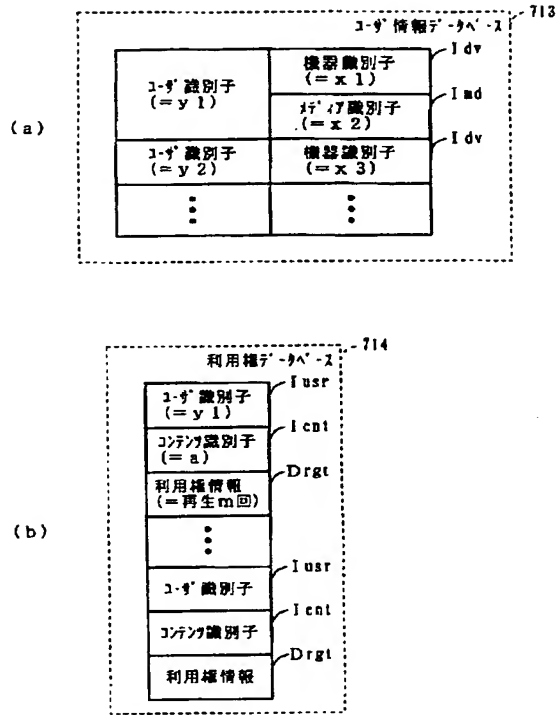
【図68】



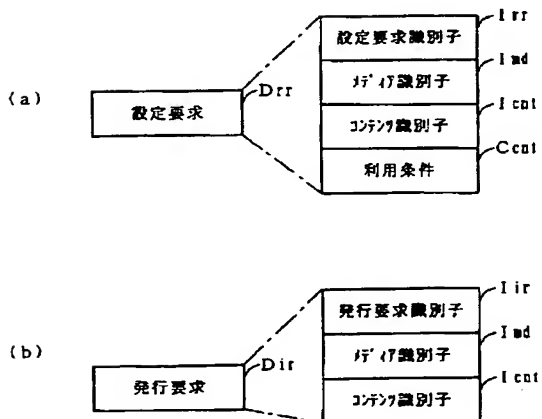
【図70】



【図71】

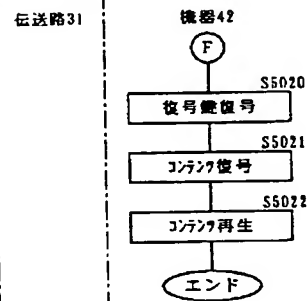


【図74】

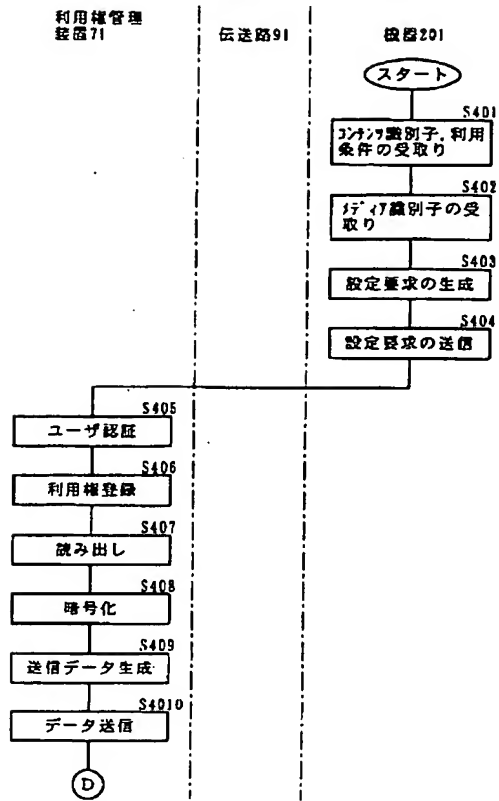


【図77】

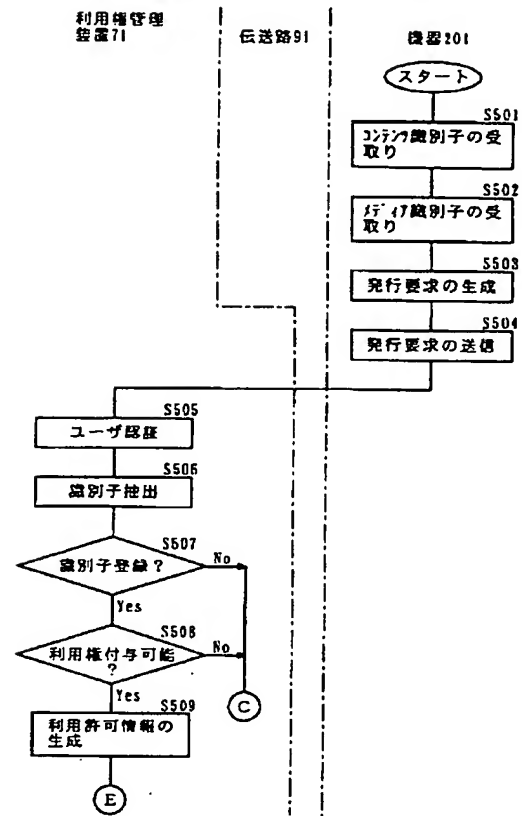
利用権管理装置11



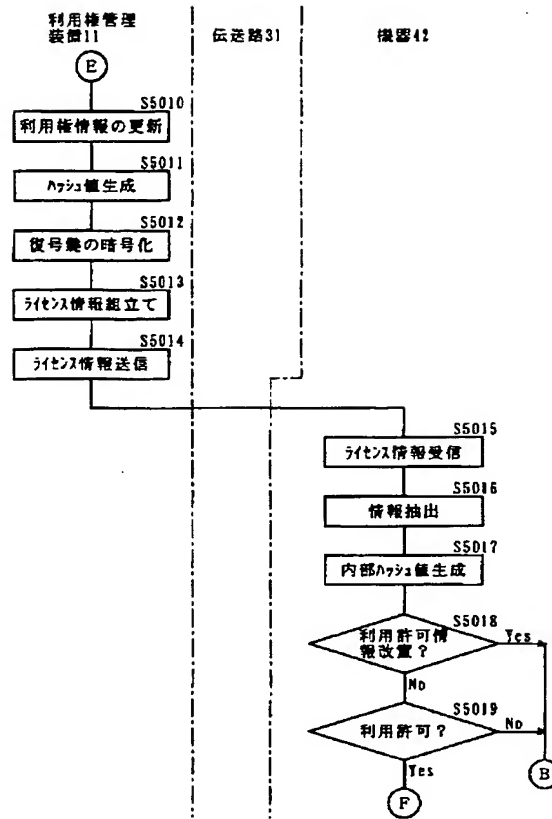
【図72】



【図75】



【図76】



フロントページの続き

(51)Int.Cl.	識別記号	F I	キーワード (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B
9/32			6 7 3 B
(72)発明者 山本 雅哉		(72)発明者 徳田 克己	
大阪府門真市大字門真1006番地 松下電器		大阪府門真市大字門真1006番地 松下電器	
産業株式会社内		産業株式会社内	
(72)発明者 岡本 隆一		(72)発明者 井上 光啓	
大阪府門真市大字門真1006番地 松下電器		大阪府門真市大字門真1006番地 松下電器	
産業株式会社内		産業株式会社内	
		F ターム (参考)	5B017 AA06 BB09 BB10 CA09 CA16
			5B085 AE03 AE29 EA06 BG02 BG03
			BG04 BG07
			5J104 AA08 DA03 NA12 PA07 PA10